UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOCELYN TROELL, individually, and for the estate of STEPHEN TROELL, *et al.*, Plaintiffs, -v- BINANCE HOLDINGS LIMITED, *et al.*, Defendants.	**Case No.: 1:24-cv-07136 (JAV)**

PLAINTIFFS' MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

In 2023, following a years-long investigation, the U.S. government revealed that Binance Holdings Limited (BHL or Binance), operator of the world's largest cryptocurrency exchange, and its founder and CEO, Changpeng Zhao, systematically flouted U.S. laws designed to prevent terrorist finance and money laundering. This case shows the human cost of that lawlessness. Plaintiffs are U.S. nationals and their family members who were killed, tortured, taken hostage, or otherwise injured in terrorist attacks committed between 2017 and 2024 by Hamas, Hezbollah, ISIS, al-Qaeda and other designated Foreign Terrorist Organizations (FTOs). Their Amended Complaint details how Defendants' deliberate decisions to service terrorist-linked accounts—even after receiving explicit warnings about their nature and the likely consequences—enabled these FTOs to access and move the funds needed to carry out the attacks that devastated Plaintiffs' lives.

Specifically, Plaintiffs allege that Defendants aided and abetted the attacks by actively and persistently enabling terrorist finance involving cryptocurrencies, which provided the terrorists with the resources they needed to attack Americans. This included facilitating over *one hundred million* dollars in unlawful transactions for people associated with Hamas, al-Qaeda, Palestinian Islamic Jihad (PIJ), ISIS, and other designated FTOs. It also included facilitating wholesale sanctions violations, to the tune of *billions* of dollars, by people and businesses acting on behalf of the Islamic Revolutionary Guard Corps (IRGC)—also an FTO—as well as others in Iran that openly and notoriously sponsor anti-American terrorism around the world (described in the complaint as the "Terrorist Sponsors"). Defendants also entered multiple conspiracies with terrorist organizations, including agreements to undermine U.S. sanctions on Iran and to facilitate terrorists' access to the proceeds of their terrorist activity. Finally, Defendants committed acts of international terrorism by providing material support to a cyber-terrorist organization that executed a ransomware attack on an Alabama hospital that killed an infant.

Defendants' misconduct violated the Anti-Terrorism Act (ATA), 18 U.S.C. § 2333, as amended by the Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. No. 114-222, 130 Stat. 852 (2016). As its codified language explains, JASTA seeks "to provide civil litigants with the broadest possible basis … to seek relief against" anybody that has "provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States." JASTA § 2(b). This includes those who act "knowingly or recklessly," and support terrorism "directly or indirectly," *id*. § 2(a)(6), including those who assist "foreign terrorist organizations, acting through affiliated groups or individuals, [to] raise significant funds outside of the United States," *id*. § 2(a)(3). "This broad liability combats terrorism by discouraging people and entities from helping others commit acts of terrorism." *Averbach v. Cairo Amman Bank*, 2025 WL 504612, at *3 (S.D.N.Y. Feb. 14, 2025).[1] More recently, Congress reiterated "that civil lawsuits against those who support, aid and abet, and provide material support for international terrorism serve the national security interests of the United States by deterring the sponsorship of terrorism and by advancing interests of justice, transparency, and accountability." Sudan Claims Resolution Act, Pub. L. No. 116-260, div. FF, tit. XVII, § 1706(a)(1), 134 Stat. 3294 (2020).

Binance and its U.S. affiliate, BAM Trading (BAM or Binance US) seek dismissal of the complaint. The motions should be denied. Defendants base many arguments on *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023), which held that social media companies that failed to prevent terrorists from using their generally available, largely unregulated platforms were not liable for aiding and abetting a terrorist attack. But Defendants misunderstand the import of *Twitter*—which turned on its distinct facts involving (1) passive inaction (2) by defendants who lacked any duty to

[1] Unless otherwise stated, internal quotation marks, citations, footnotes, and markup are omitted from materials quoted in this Memorandum.

act (3) while providing routine services. But *Twitter* did not overrule *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021), which sustained a JASTA claim against a bank that actively assisted terrorist finance. In *Twitter*'s wake, courts evaluating claims involving active assistance by regulated financial institutions have sustained them under *Twitter* and *Kaplan*. *See, e.g.*, *Henkin v. Kuveyt Turk Katilim Bankasi A.S.*, 2025 WL 622546, at *3-5 (E.D.N.Y. Feb. 26, 2025); *Hakimyar v. Habib Bank Ltd.*, 2025 WL 605575, at *9-10 (S.D.N.Y. Feb. 25, 2025); *Lelchook v. Lebanese Canadian Bank*, 2024 WL 967078, at *6 (S.D.N.Y. Mar. 6, 2024); *Bonacasa v. Standard Chartered PLC*, 2023 WL 7110774, at *11 (S.D.N.Y. Oct. 27, 2023); *King v. Habib Bank Ltd.*, 2023 WL 8355359, at *2 (S.D.N.Y. Dec. 1, 2023). This is such a case.

The Court need not take our word for this—but can instead rely on a recent on-point decision. In *Raanan v. Binance Holdings Ltd.*, 2025 WL 605594 (S.D.N.Y. Feb. 25, 2025), brought by victims of the October 7 attack based on Binance's assistance to Hamas and PIJ, Judge Koeltl described the plaintiffs' allegations as "comparable" to *Kaplan* and held that they "capture the 'essence' of aiding-and-abetting liability: that Binance and Zhao 'consciously and culpably participated in Hamas's and PIJ's wrongdoing.'" *Id*. at *22-23 (quoting *Twitter*, 598 U.S. at 504, 506). "[T]he defendants' alleged widespread, intentional circumvention of anti-terror financing regulations, considered with the defendants' purported knowledge that Hamas and PIJ were transacting on the Binance platform, support the inference that defendants' assistance was knowing. And the financial assistance allegedly provided was substantial, even if not directly targeted at the October 7 attacks in particular." *Id*. at *23. The allegations here are stronger than those sustained in *Raanan*: Plaintiffs allege, in even greater detail than the complaint in *Raanan*, how Binance's willful unlawful acts enabled horrific terrorist violence. For the reasons set forth in *Raanan* and this Memorandum, this Court should deny the motions to dismiss.

PLAINTIFFS' ALLEGATIONS

I. Binance Actively Assisted Foreign Terrorist Organizations And Iran's Terrorist Sponsors In Their Criminal Activity

Since it began operations in 2017, Binance ***actively*** catered to terrorist groups and their supporters in multiple ways. *First*, Binance refused to implement required anti-terrorism controls and sabotaged the limited controls it had. Although U.S. law required Binance to implement a robust anti-money laundering (AML) program—including Know Your Customer (KYC) policies, transaction monitoring and blocking, and regulatory reporting through Suspicious Activity Reports (SARs)—Binance had *no* program *at all* for its first year. ¶¶506-08. When Binance finally implemented a program, it was "paper thin," ¶526, with "categorical gaps that rendered it ineffective against terrorist finance," ¶507. For example, rather than adopt comprehensive KYC requirements, Binance allowed the "vast majority" of users to move substantial sums of cryptocurrency without even providing their *names* until May 2022. ¶¶516-18, 524-26. Binance also advertised that it was screening transactions based on users' locations (to stop users from sanctioned countries from using the platform)—but actively encouraged users in prohibited jurisdictions to use virtual private networks (VPNs) to mask their location and evade Binance's controls. ¶¶520, 754. And when Binance identified suspicious transactions, it refused to file required SARs with U.S. authorities. ¶¶16, 19, 500, 761, 1258. "Binance allowed millions of suspicious transactions to proceed," without filing a single SAR through at least May 2022. ¶527.

Binance also embraced customers and products that were particularly well-suited to terrorist finance—including cryptocurrency mixers (which commingled cryptocurrency deposits to obscure the sources and destinations of funds), anonymity-enhanced cryptocurrencies, nested exchange sub-accounts, and darknet users. ¶¶530-32, 698-708. This misconduct was not a mere failure to act; instead, as the government found, it was "the product of *deliberate choices* by senior

management." ¶751; *see also* ¶641 (attributing misconduct to Zhao). "Defendants thus maintained a deliberately ineffective KYC and blocking policy precisely so that Binance could court prohibited customers who otherwise would avoid the platform. That deliberate policy choice directly enabled Hamas, Hezbollah, PIJ, and the IRGC to use the Binance platform to fund and commit terrorist attacks on Americans, including Plaintiffs." ¶639.

Second, Binance actively enabled transactions involving terrorist organizations, as well as transactions that it knew violated anti-terrorism sanctions. Thus, Binance caused funds to flow *directly* to the FTOs that committed many of the attacks at issue. As the Treasury Department reported, "Binance user addresses were found to interact with bitcoin wallets associated with ISIS, Hamas' Al-Qassam Brigades, Al Qaeda, and the Palestinian Islamic Jihad." ¶631. From July 2017 through July 2023, Binance facilitated hundreds of transactions for millions of dollars for users associated with these FTOs, as well as the IRGC and others. ¶¶501-02. Based on a "conservative" estimate, Binance "helped Hamas obtain at least *$56 million* through transfers," ¶1263, and performed transactions "for dozens of users with 'tens of millions of dollars in transactions with an identified PIJ network,'" ¶1265. *See also* ¶¶1256-78 (additional allegations showing substantial illicit transactions by Hamas and PIJ). Similarly, Binance enabled a substantial volume of transactions for al-Qaeda, ¶¶1391-93, ISIS, ¶¶1487-89, and Hezbollah, ¶¶1152-58. Plaintiffs' estimates are derived from their review of publicly available cryptocurrency wallet attribution and transaction data, analyzed using industry-standard techniques. *See* ¶¶768-770. But this analysis covers only transactions reported on public blockchains. *E.g.*, ¶¶735, 771, 1263-64, 1268, 1394, 1490. Discovery will reveal additional private transactions among Binance users involved with the terrorist groups at issue—which were visible to Binance, but obscured to others. ¶535.

Binance also caused funds to flow to FTOs *indirectly* by enabling wholesale violations of anti-terrorism sanctions on Iran's Terrorist Sponsors. ¶¶503-04. The Terrorist Sponsors included the Foundation for the Oppressed, the IRGC, Hezbollah, and Supreme Leader Ayatollah Ali Khamenei and his office (the SLO). ¶63. Beginning even before the Islamic Revolution of 1979, and continuing through this day, these organizations collectively built a robust, widespread, and cohesive terrorist funding, planning, and logistics network to attacks Americans, provoking sanctions from the United States. ¶¶66-161. These entities were the most important sponsors of terrorist attacks committed by the FTOs involved in this case, such that "[a]t least one Terrorist Sponsor played a direct role in every attack where Plaintiffs (or their loved ones) were killed, kidnapped, and/or maimed," and "most attacks prominently featured support from many, if not all, of the Terrorist Sponsors." ¶165; *see also* ¶¶166-400 (providing details). Among other facts, Plaintiffs explain, by reference to authoritative statements from governments, the United Nations, and terrorism scholars, that the Terrorist Sponsors seized control of large swaths of the Iranian economy, including specific strategically important sectors, and converted the profits from those sectors into fuel for anti-American terrorist violence by FTOs like Hezbollah and Hamas. ¶¶401-98.

The scale of Binance's violations benefiting the Terrorist Sponsors was dramatic—involving "nearly $8 billion in transactions with Iranian counterparties." ¶¶18, 580, 759-65. In the beginning, Binance brazenly enabled transactions that violated U.S. sanctions laws—performing no required screening whatsoever. ¶¶507, 522-23, 528. Later, while trying to give the appearance of compliance, Binance continued to knowingly facilitate sanctions violations. Thus, even after employees identified "more than 12,500 users who had provided Iranian phone numbers," Binance maintained those accounts—while externally claiming "that it had blocked all Iranian customers."

¶526. Indeed, while Binance was purporting to block transactions by sanctioned users, internal communications reveal that it was secretly courting them and celebrating their use of the platform. ¶¶752, 756-57. This use included transactions involving IRGC fighters and supporters, ¶¶766-76, IRGC cryptomining operations, ¶782-85, IRGC ransomware operations, ¶¶777-81, and Nobitex, a cryptocurrency exchange in Iran that was a front for the IRGC and masked its users (including IRGC agents), ¶¶580, 763-65.[2] Binance also enabled IRGC money laundering by helping its users trade in Iranian cryptocurrencies purpose-built to evade sanctions. ¶¶709-15. All of this was done knowingly. Binance's internal communications showed that its senior management was aware of ongoing sanctions violations, and was committed to maintaining the Iran-facing business covertly. ¶¶750-52. The government found that "Zhao knew that his decision not to implement an effective AML program would result in Binance facilitating transactions between U.S. users and users in Iran … in violation of U.S. law." ¶641. And Binance's (now former) Chief Compliance Officer admitted internally in 2018 "that Binance's customer service employees were 'teaching ppl how to circumvent sanctions' and openly worried about 'land[ing] in jail.'" ¶643.

Third, Binance actively deceived governments and the public to assist its terrorist customers. *See* ¶¶635, 640(d). For example, upon learning that Hamas-associated entities were using its platform, Binance "attempted to influence the third-party service provider that reported on Binance's conduct, attempting to conceal the wrongdoing." ¶¶636, 1258. And in 2019, when Binance identified accounts associated with "ISIS and Hamas," it allowed the "terrorist owners"

[2] Among Binance's Iranian customers, Nobitex stands out. It was Iran's largest cryptocurrency exchange, and "was dominated by, controlled by, and/or a front for Terrorist Sponsors," with shareholders who were closely connected to the Terrorist Sponsors and public advocates for anti-American terrorism. ¶¶483-92. The exchange guided users to evade sanctions on Iran. ¶¶493-94. Binance did a tremendous volume of business with Nobitex—billions of dollars in transactions—allowing the Terrorist Sponsors to access the global financial markets in violation of anti-terrorism sanctions. ¶¶495, 580, 763-64.

of the accounts to retain access and "withdraw the balance" rather than shutting them down. ¶¶637, 1259. These examples were "part of a pattern" whereby, if law enforcement froze a Binance user's account (including for terrorism concerns), then "as soon as the account was unfrozen," Binance employees would alert the user. ¶638. The team was instructed not to "directly tell the user to run," but instead reveal the investigation and hope they "will get the hint." *Id*. Often, Binance then gave those same users another account. *See* ¶635.

Binance also lied about its business and compliance activities. ¶640(c)-(d). Outwardly, Binance and Zhao trumpeted the need to strictly adhere to the letter and spirit of sanctions laws. ¶¶647-59. Those statements were false when made, as Binance and Zhao knew they were actively circumventing anti-terrorism sanctions. And when financial institutions and regulators expressed concerns about Binance's foreign customer base, Binance's executives lied, falsely insisting they screened and blocked sanctioned users. ¶¶528-29, 753, 755.

In 2019, Binance played a new gambit to deceive U.S. authorities. Binance falsely asserted that it was no longer allowing U.S. users to access its main cryptocurrency exchange on Binance.com. It did this to shield Binance.com from U.S. regulatory scrutiny, including by counterterrorism authorities. ¶522. Zhao understood (in his own words) that "[t]he United States has a bunch of laws to prevent you and Americans from any transaction with any terrorist," which apply if Binance "serve[s] Americans or service[s] U.S. sanctioned countr[ies]." *Id*. To evade counterterrorism authorities, Binance announced that it was blocking all U.S. users from Binance.com, and routing them instead to a regulated exchange nominally operated by defendant Binance US. ¶521; *see also* ¶¶31-34. In fact, Binance.com surreptitiously retained much of its vast U.S. user base. "As of January 2020, approximately 19.9 percent of [Binance.com's] customers were located in the United States." *Id*. This included millions of users. ¶1567.

Instead of being truly independent, the U.S. exchange was a fig leaf designed to conceal and enable Defendants' ongoing violations of U.S. law. Defendants used the U.S. exchange "as a laboratory to see which customers would trade high volumes" before migrating high-volume customers to Binance.com. ¶514. Binance US was also intended to—and did—divert U.S. regulatory attention away from Binance.com. ¶¶684-85, 687, 691. Thus, Defendants' "public proclamations … that Binance US was independent and that it controlled the operations of the U.S. Exchange … were lies. In reality, nearly every material aspect of Binance US's operations was tightly controlled by Zhao and Binance, often in ways that made a mockery of the corporate form." ¶690. Thus, Binance and Zhao controlled Binance US's bank accounts (and thus Binance US customers' funds), ¶693, as well as the U.S. exchange's cryptocurrency assets, ¶694, its data, ¶695, and even its routine business expenditures, ¶696. Internally, Binance US employees "referred to Zhao's and Binance's control of its operations as 'shackles' that impeded Binance US employees from actually being able to run the U.S. Exchange." ¶697. Binance US's first CEO stated that the degree of control exercised by Binance and Zhao made her entire team feel "duped into being a puppet." Binance US's second CEO "resigned just a few months into the job," and "later testified: '[W]hat became clear to me at a certain point was [Zhao] was the CEO of [Binance US], not me." *Id*. Based on these allegations, Plaintiffs allege that "Binance US Effectively Functioned as Binance and Zhao's Alter Ego." Complaint p.239 (section heading 2). At a minimum, Binance US was "part of a common enterprise with Zhao and Binance," ¶1578, and its "*raison d'etre* was to serve as an instrument that Binance and Zhao could (and did) use to influence the conduct of U.S. government officials," ¶1579. This, in turn, was "a critical part of [Defendants'] integrated scheme to … forestall regulation of Binance's illegal activities and deflect the attention of U.S." officials "away from Binance and its illegal activities." ¶1580.

II. Binance's Misconduct Was Conscious And Culpable

Binance's misconduct was ***conscious and culpable***, not ignorant or innocent. Binance consciously sought to maximize its share of the illicit market, and revenue from those sources. *E.g.*, ¶3098. Communications among managers showed that Binance knew that it was breaking many laws and enabling illicit transactions for terrorists and other criminals. ¶752; *see also* ¶¶511-15, 517, 522, 528-29, 632-35, 637-38, 643 (additional communications showing consciousness of guilt). The violations were a business decision: Zhao "believed that implementing robust KYC requirements would deter users from joining Binance's platform, thus decreasing Binance's transaction volume and therefore its revenues." ¶639. Binance thus "maintained a deliberately ineffective KYC and blocking policy precisely so that Binance could court prohibited customers who otherwise would avoid the platform." *Id.*; *see also* ¶505. Binance even touted its noncompliance to "VIP customers as a market differentiator." ¶731.

Binance also knew that many of the transactions it was processing were not run-of-the-mill cryptocurrency transactions, but were instead laundering the proceeds of crime. In a chat conversation, a Binance compliance employee wrote "that Binance needed 'a banner' that stated, 'is washing drug money too hard these days – come to Binance we got cake for you.'" ¶634. In another chat, Binance's Chief Compliance Officer opined of Binance's customers, "Like come on. They are here for crime." *Id*. In 2018, the Chief Compliance Officer acknowledged internally that there was "no fking way we are clean," admitting that "Binance's customer service employees were 'teaching ppl how to circumvent sanctions,'" and openly worrying about "land[ing] in jail." ¶643. Binance also permitted users of the notorious darknet Hydra Market—whose "offerings included ransomware-as-a-service, hacking services and software, stolen personal information, counterfeit currency, stolen virtual currency, and illicit drugs"—to transact on Binance. ¶706. And it allowed nested exchanges, notorious for assisting in "money laundering, scammers, and

ransomware payments," to do the same. ¶700. Even when a customer from these tainted sources was identified, Binance's position was to let the customer "know to be careful with his flow of funds, especially from darknet." ¶708. Rather than ban those users, the company's stance was that they could "come back with a new account" because "Offboarding = bad in [Zhao's] eyes." *Id*.

Binance knew the nature of its terrorist customers. The company deployed "a robust suite of internal tools" and advertised partnerships with elite blockchain analysis firms to track customers and monitor transactions. ¶¶662, 665-73, 769-70. This ensured that Binance "knew the identities of users, including designated terrorists, who were operating on the Binance exchange." ¶664. Indeed, the specific firms Binance retained issued public reports calling out the terrorist financing risks inherent in cryptocurrency transactions—and certainly provided even more information privately to Binance. ¶¶666-71. Mainstream and trade publications likewise observed that terrorist organizations were making prolific use of cryptocurrency for fundraising. ¶¶565, 568-81, 750-93, (IRGC); ¶¶587-94, 1269-78 (Hamas and PIJ); ¶¶1481-99, 603-06 (al-Qaeda and ISIS). And Binance knew of accounts associated with specific terror groups. *E.g.*, ¶¶636-37 (alleging Binance's knowledge of "accounts associated with the terrorist groups ISIS and Hamas"); ¶¶767, 1263, 1266-67, 1393, 1489 (alleging that Binance knowingly assisted wallets identified with the IRGC, Hamas, PIJ, al-Qaeda, and ISIS).

Binance also knowingly and systematically facilitated transactions with Iran. Internal communications among senior Binance employees, including the Chief Compliance Officer and Deputy Head of Compliance show that although Binance's public "stance [was] [n]ot to openly do business with Iran due to sanctions … we still support [I]ranian customers but that has to be done non-openly." ¶752. Similar discussions over a substantial period of time showed an ongoing effort to covertly serve Iranian customers in violation of sanctions. *See* ¶¶752-53, 755-62. And indeed,

the sheer volume of Binance transactions serving Iranian customers—well over a million transactions involving billions of dollars, ¶¶759-65—supports a strong inference that the company and its senior management knew.

Binance also knew that its actions enabled terrorist violence. ¶¶536-628. As early as 2008 the U.S. government warned that "[d]igital currencies … are vulnerable to money laundering and terrorist financing." ¶542. Thereafter, "[a] steady drumbeat of official warnings came from the U.S. government, the United Nations, the Financial Action Task Force," the media, and industry groups "that terrorist groups were actively looking to use—and did in fact use—cryptocurrency to fund their operations and commit attacks." ¶537; *see, e.g.*, ¶¶543-47, 555, 562, 1483-85. For example, in October 2018, FinCEN "explicitly connected Iran's embrace of cryptocurrencies to its support for the IRGC and its terrorist proxies," warning that Iran "may seek to use virtual currencies" "to fund the regime's nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well as to Lebanese Hizballah, Hamas, and other terrorist groups." ¶570. Earlier that year, the U.S. National Security Advisor gave a widely reported speech explaining that "[w]hen you invest in Iran, you're investing in the IRGC. You might as well cut the Islamic Revolutionary Guard Corps a check and say, 'please use this to commit more murder across the Greater Middle East.'" ¶824.

These were but a handful of the public and private warnings Binance received explaining that terrorist financiers—including ones specifically associated with the terrorist groups in this case—were seeking the path of least resistance (*i.e.*, least oversight) through the international financial system, and were therefore eager to use tools or platforms that allowed them to move large volumes of money quickly and secretly across the world. *E.g.*, ¶609 (explaining that "[i]llicit

actors continuously seek out the weakest links in the chain"); *see also* ¶¶607-08, 719-38. Authoritative sources also informed Binance that terrorists could wreak havoc with even small sums of money. ¶¶739-46. Indeed, Binance's own executives understood this, as evidenced by an internal exchange where Binance's Chief Compliance Officer explained to a colleague that "terrorists usually send small sums." ¶633.

Other businesses heard these warnings and treaded carefully. *E.g.*, ¶645 (documenting how prominent tech companies backed away from Iran). The former CEO of Goldman Sachs, for example, was skeptical of cryptocurrency precisely because "[y]ou don't know whether you're paying the North Koreans or Al Qaeda or the Revolutionary Guard." ¶642. Aware of the heightened risk, other cryptocurrency exchanges implemented robust internal controls and filed tens of thousands of SARs flagging suspicious transactions flowing through their systems. ¶612. Binance did the opposite, willfully opening the floodgates to instant, pseudonymous global transfers—and thus claiming a huge share of the illicit market.

To the extent Binance was ignorant of any material fact, that ignorance resulted from willful blindness tantamount to actual knowledge. ¶¶674-80. As Binance's former Chief Money Laundering Officer explained, Binance's approach was to "see the bad, but we close 2 eyes." ¶¶634, 680. Binance did not merely fail to satisfy its legal obligations, but instead deliberately shirked those obligations with contempt for the policies underlying them. Tellingly, Defendants' motions do not address these allegations at all.

Finally, Binance's misconduct caused it to be prosecuted alongside Zhao, resulting in criminal guilty pleas by both as well as resolutions with multiple agencies. *E.g.*, ¶13. These resolutions included the largest civil monetary penalty in the history of FinCEN and OFAC. ¶631. Innocent mistakes and garden-variety regulatory lapses do not garner such penalties.

III. Binance's Unlawful Acts Enabled The Attacks That Injured Plaintiffs And Their Loved Ones

Defendants' misconduct ***enabled the attacks*** that injured Plaintiffs and their loved ones. As explained *supra*, Binance facilitated myriad transactions for customers associated with the designated FTOs that attacked Plaintiffs and their loved ones, as well as for the benefit of the Terrorist Sponsors, all of which caused millions of dollars to flow through to the terrorists that committed the attacks. Providing these terrorists with access to millions of dollars foreseeably risked terrorist violence against Americans because "[m]oney is the lifeblood of terrorism." ¶719. In the words of the Department of Justice, "Binance's and Zhao's willful violations of anti-money laundering and sanctions laws threatened the U.S. financial system and our national security." ¶6. "Defendants gave uniquely dangerous actors (FTOs) access to a uniquely dangerous product (cryptocurrency) on a uniquely dangerous platform (Binance's exchange)—which these terrorists used to finance attacks." ¶716.

The United States, other governments, the United Nations, NGOs, think tanks, and terrorism scholars have all publicly explained that anybody who participates in terrorist finance foreseeably contributes to terrorist violence against Americans. *E.g.*, ¶¶607-19. They specifically admonished cryptocurrency exchanges and financial institutions to act as a "first line of defense" against terrorist finance. ¶615. And they emphasized that providing even small amounts of money would enable horrific violence against Americans. ¶¶739-46. Indeed, the warnings showed that average terrorist attacks cost only about $2,700 to carry out, meaning that "the millions in dollars in value that Defendants flowed to the FTOs here was more than enough to fund thousands of attacks—sufficient to kill every Plaintiff in this case multiple times over." ¶745.

In addition to these clear warnings against terrorist finance—which alerted all financial institutions of the risks of opening their platforms to terrorists—authoritative warnings specifically

called out the risk of providing access to cryptocurrencies to the terrorist groups that planned, authorized, and committed the attacks in this case. *See, e.g.*, ¶¶536-628, 718-48, 788-97, 817-34, 1260-78, 1391-98, 1481-85. Access to global cryptocurrency exchanges like Binance provided at least eight different benefits to terrorist organizations, including: (1) global reach and unrivaled ease of transferring funds across international borders; (2) encryption and anonymity; (3) secure, digital, and ready stores of value; (4) near-instantaneous transaction speed; (5) a back door to the U.S. financial system; (6) the ability to access currency on mobile phone networks in conflict zones; (7) an off-ramp to fiat currency; and (8) a closed ecosystem free from public and regulatory oversight. ¶¶723-38. In other words, by providing access to cryptocurrency transactions, Binance gave the terrorists an unprecedentedly convenient way to raise, move, and spend money while avoiding the regulations and oversight that would have prevented them from doing so through the traditional financial system. These extra benefits acted as "a force multiplier" enabling the terrorists to more easily route money to fund attacks. ¶722.

Public warnings also explained how the Terrorist Sponsors—including the Supreme Leader's Office, Hezbollah, the Foundation for the Oppressed, and the IRGC—exercised end-to-end control over Iran's cryptocurrency ecosystem. The Terrorist Sponsors had monopoly control over key sectors of the Iranian economy—including cryptocurrency, finance, telecommunications, data processing, and sanctions evasion—such that by participating in and enabling those sectors, Binance's unlawful activities caused money to flow through to the Terrorist Sponsors, who used that money to finance attacks on Americans in the Middle East. ¶¶401-98. The allegations trace the entire chain of value, showing how cryptocurrency transactions through Binance caused money to flow to the Terrorist Sponsors, and further explaining how the Terrorist Sponsors used those

funds to finance the specific weapon types, terrorist groups, and individuals that attacked Plaintiffs. ¶¶563-84, 620-28, 676-78, 772-76, 786-1150, 1160-1254, 1279-1468, 1515-48.

Binance's misconduct assisted the Terrorist Sponsors directly and indirectly. On the direct side of the spectrum, Binance: (1) provided a profitable outlet for Iranian cryptocurrency mining operations, which Terrorist Sponsors controlled, ¶¶788-99; (2) provided an essential bridge to the global financial system for Iranian cryptocurrency exchanges, thus allowing profits from cryptocurrency trades to flow to the Terrorist Sponsors, ¶¶814, 479-98; (3) provided profits to specialized Iranian cybertechnology firms, which provided the technology necessary for Iran's blockchain and were controlled by the Terrorist Sponsors, ¶815-16; and (4) allowed IRGC members to trade cryptocurrencies for the benefit of the Terrorist Sponsors, ¶813. Less directly, Binance's deliberate provision of extensive cryptocurrency services to Iranian customers caused profits to flow to: (1) the Central Bank of Iran, ¶800, which was captured by the Terrorist Sponsors, ¶¶416-23; (2) telecommunications firms that provided the data services for cryptocurrency mining and transactions, which were owned fronts of the Terrorist Sponsors, ¶¶801-07; and (3) the power generation sector, which was likewise owned by the Terrorist Sponsors, ¶¶808-12.

Once the Terrorist Sponsors absorbed the profits from Binance's misconduct, they spent that money to finance terrorist attacks on Americans. "Plaintiffs allege that more than half of all such dollars foreseeably enabled Iranian-sponsored attacks." ¶817. Since 2003, the Iranian government has had in place a "Logistics Policy Directive" requiring a share of profits from IRGC-affiliated commercial enterprises to be spent to advance IRGC operations—including support for terrorism by the groups that attacked Plaintiffs. ¶¶818-22. U.S. government officials have confirmed that the Terrorist Sponsors use their domination of the Iranian economy "to finance terrorist attacks by proxy groups." ¶823; *see also* ¶¶824-29. These sources made clear that the

Terrorist Sponsors "prioritize[] … buying guns and bombs for foreign terrorists" over shoring up the Iranian economy or other benign ends, ¶828(a), such that "any dollar they get … will be used for the IRGC before it's ever used for their people," ¶828(b). In other words, "we must operate under the assumption that every dollar made available to Iran is another dollar that will be used to put U.S. servicemembers in harm's way or threaten our allies, especially Israel …. [A]ny money to Iran supports terrorism." ¶828(c).

Plaintiffs detail how the direct and indirect profits from Binance's misconduct vis-à-vis Iran benefited the Terrorist Sponsors' terrorist activities—including IRGC operations, ¶¶830-34, the Khamenei Cell (which included the leadership of the Supreme Leader's Office, the Foundation for the Oppressed, Hezbollah, the IRGC, and other terrorists), ¶¶835-950, terrorist logistics cells, ¶¶951-74, incentive and reward payments for terrorists and their families, ¶¶975-86, as well as weapons and logistics (including missiles, rockets, mortars, drones, rocket propelled grenades, small arms, communications technologies, electronic warfare systems, and others), ¶¶987-1148. The complaint further explains how those Terrorist Sponsors supported terrorist attacks by the FTOs that killed and injured Plaintiffs and their loved ones, drawing lines from each sponsor to each FTO, including specific terrorists and geographies involved in the attacks. ¶¶1149-1514.

Importantly, although Plaintiffs' allegations of causation are broad, they are not blunderbuss. As Plaintiffs explain, they "do not allege that the IRGC monopolized every—or even most—segments of Iran's economy." ¶410. Instead, the IRGC's monopolies (as opposed to mere influence or presence) included the sanctions evasion, finance, import/export, and communications and Internet technology sectors. ¶411. Similarly, Plaintiffs "do not allege that Defendants' resources aided such attacks enabled by any IRGC or SLO component anywhere in the world." ¶1151. Instead, the allegations are focused on the specific subset of terrorist groups, attack types,

and geographies that received critical resources as a result of Defendants' misconduct. *See id.*; *see also* ¶1498-99 (similar disclaimer with respect to ISIS). Similarly, as Binance US points out, Plaintiffs do not allege that all of Iran's 85 million citizens were terrorist collaborators; but Plaintiffs do allege (and Defendants ignore) that approximately 1.5% of Binance's individual users in Iran (potentially hundreds of thousands of people) were IRGC members, ¶¶772, 774—to say nothing of its large business customers like Nobitex that transacted incredible volumes.

The foregoing causal chains were detailed in public sources that were readily available to Defendants before and contemporaneously with their misconduct—as well as in private intelligence that any business in Defendants' position would have. Plaintiffs accordingly allege not only that Defendants' misconduct caused terrorist attacks—but that Binance engaged in misconduct knowing that terrorist attacks on Americans would result.

IV. Plaintiffs Seek Relief Under The Anti-Terrorism Act

Based on the foregoing factual allegations, Plaintiffs assert five claims for relief. *First*, all Plaintiffs assert a cause of action for aiding and abetting terrorist attacks that were planned, authorized, or committed by designated FTOs. ¶¶3041-51. This claim alleges that by providing critical financial support that enabled the attacks, Defendants aided and abetted those attacks.

Second, all Plaintiffs other than those injured by ISIS assert a conspiracy claim based on Binance's participation in the Terrorist Sponsors' counterpressure conspiracy. ¶¶3052-3132. This count alleges that the Terrorist Sponsors engaged in a long-term effort to weaken U.S. resolve to maintain anti-terrorism sanctions on Iran through two means: (1) by demonstrating that the sanctions were ineffective through circumvention; and (2) by retaliating against the United States for imposing sanctions via terrorist attacks—with the overall objective being to secure the repeal of sanctions. Defendants joined this conspiracy by assisting in widespread sanctions evasion, hoping to profit from the end of sanctions on Iran by quietly growing an early foothold in that

market primed to grow rapidly when sanctions were lifted. ¶¶3055, 3098-110. This was more than mere parallel conduct: it was the product of an agreement between, at least, Defendants and Nobitex, a major Iranian customer that was also an IRGC front and participant in the conspiracy. ¶¶3057-61. The attacks furthered that conspiracy because they, too, were intended to erode the U.S. commitment to sanctions. ¶¶3062-97, 3111-20.

Third, all Plaintiffs other than those injured by ISIS allege that Defendants entered into a conspiracy led by the IRGC and joined by multiple FTOs, "whose overall object was to maintain each such FTO's ability to access the payments they received in connection with their hostage-taking, human trafficking, ransomware, and protection payment schemes." ¶3134; *see* ¶¶3133-66. Here, Defendants sought to profit by operating as the financial back-office allowing the terrorists to reap the economic rewards of their terrorist activity, and to spend those funds to promote further violence.

Fourth, the ISIS victim Plaintiffs assert that Defendants conspired to provide material support to ISIS, and that the resulting attacks were acts in furtherance of that conspiracy. ¶¶3167-78. The support took the form of money, and of structuring transactions to disguise the monetary support. ¶3168.

Finally, two Plaintiffs assert that Defendants committed an act of international terrorism by processing payments to a ransomware organization called Wizard Spider, which carried out a cyberattack on an Alabama hospital that resulted in the death of an infant child. ¶¶3179-87.

STANDARD OF REVIEW

To survive a motion to dismiss, a complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The Court must accept all factual allegations as true and draw all reasonable inferences in Plaintiffs' favor. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

ARGUMENT

Defendants' merits arguments rest principally on three flawed propositions. *First*, Defendants assert that Plaintiffs seek to impose liability for "routine" services. BHL Mem. 2, 14, 19-22, 27; BAM Mem. 14-16. Is this a joke? The complaint alleges that "none of Defendants' culpable conduct constituted routine business activity" because "Defendants knowingly and intentionally deviated from all norms of routine business behavior." ¶630. Indeed, Defendants paid *over $4 billion in penalties* for merely a *subset* of the misconduct alleged in Plaintiffs' complaint. ¶4. Defendant Zhao went to prison. *Id*. And the complaint is replete with allegations that, time and again, Defendants went out of their way—and outside the law—to: (1) attract and cater to criminal customers; (2) structure their business to help those customers evade critical anti-terrorism controls; and (3) assist identified criminal customers in avoiding detection or enforcement. *See supra* pp.4-9. Many of these acts were not only contrary to law, but also to Binance's stated policies and practices. ¶¶528-29, 646-60. Such brazen misconduct might have been "routine" at Binance—but it is certainly not properly regarded as "routine" for purposes of assessing culpability. *See Raanan*, 2025 WL 605594, at *21 (holding that the complaint against Binance alleged "more than mere passive nonfeasance in the provision of routine services"); *Kaplan*, 999 F.3d at 858 (rejecting defendant bank's "routine banking services" argument when plaintiffs alleged that the bank "violated banking regulations and disregarded its own internal policies" to assist terrorist-affiliated customers making deposits without disclosing sources of funds); *King*, 2023 WL 8355359, at *3 (holding that complaint alleged that the defendant "provided non-'routine' banking services to terrorists and their allies"). At a minimum, whether the provision of "financial services to [terrorists] should … be viewed as routine … raises questions of fact for a jury to decide," *Linde v. Arab Bank, PLC*, 882 F.3d 314, 327 (2d Cir. 2018), and so the Court must score this issue in Plaintiffs' favor at the pleading stage.

Second, Defendants insist that they cannot be liable absent allegations that Defendants *intended* to aid terrorism. BHL Mem. 1-3, 5-9, 15-16, 23, 24-25, 28; BAM Mem. 14, 17, 22-23. But Plaintiffs allege that Defendants knowingly enabled terrorists "to make, receive, and move hundreds of millions of dollars to support their terrorist operations," ¶12, aware that these same terrorists used cryptocurrency transactions to finance violence against Americans, ¶¶244, 536-628. Defendants also knew that their conduct was unlawful, and did it anyway. No additional intent is required. "There is no requirement of specific intent, and a defendant does not have to 'wish[] to bring about' an act of terrorism or 'kn[ow] of the specific attacks at issue.'" *Bernhardt v. Islamic Republic of Iran*, 47 F.4th 856, 868 n.12 (D.C. Cir. 2022) (quoting *Linde*, 882 F.3d at 329).

Instead of always requiring intent, the well-established law of aiding and abetting puts scienter and the amount of assistance on a sliding scale, "with a lesser showing of one demanding a greater showing of the other." *Twitter*, 598 U.S. at 491-92. Under this rule, intent is required in cases like *Twitter* involving "nothing more than inaction" and minimal assistance. *Monsen v. Consolidated Dressed Beef Co., Inc.*, 579 F.2d 793, 800 (3d Cir. 1978) (cited in *Twitter*, 598 U.S. at 491). But where, as here, the defendant's assistance was substantial, and its actions were not routine business, liability is appropriate even "with a minimal showing of knowledge." *Camp v. Dema*, 948 F.2d 455, 459 (8th Cir. 1991) (cited in *Twitter*, 598 U.S. at 490); *see also Monsen*, 579 F.2d at 799 (holding that where the "aider and abettor derives benefits from the wrongdoing," it is enough to show "constructive notice of intended impropriety"). Consistent with that common-law sliding scale, JASTA expressly targets those who act "knowingly or recklessly." JASTA § 2(a)(6).

Similarly, conspiracy requires agreement to do an unlawful act—but that act need not be the tort that injured the plaintiff. As long as the tort furthered the object of the agreement, liability attaches—even if the defendant "neither planned nor knew about the particular overt act that

caused injury." *Halberstam v. Welch*, 705 F.2d 472, 487 (D.C. Cir. 1983). For example, in *Halberstam*, which Congress expressly incorporated as the legal framework for JASTA liability, the defendant and her co-conspirator "agreed to undertake an illegal enterprise to acquire stolen property," which was sufficient to render the defendant liable for an unplanned murder during a botched burglary. *Freeman v. HSBC Holdings PLC*, 57 F.4th 66, 77 (2d Cir. 2023). Moreover, the existence of an agreement can be proved—and certainly alleged—based on circumstantial facts. *See Relevant Sports, LLC v. U.S. Soccer Fed., Inc.*, 61 F.4th 299, 306 (2d Cir. 2023). Here, Plaintiffs allege multiple unlawful conspiracies including Defendants and the terrorists who attacked Plaintiffs, and explain why the attacks furthered each conspiracy's objectives.

Third, Defendants fault Plaintiffs for failing to show that the specific funds and resources Defendants allowed the terrorists to obtain were used in the specific attacks that injured Plaintiffs. BHL Mem. 1, 3, 9, 11-12, 16-17, 19, 29; BAM Mem. 17. This nexus argument fails. Plaintiffs allege that Defendants' unlawful acts assisted the attacks that injured Plaintiffs. *See, e.g.*, ¶¶3, 20, 536, 639, 722, 787, 835, 875-77, 885, 986-88, 990-91, 1150, 1192, 1201-02, 1216-18, 1250, 1255, 1284, 1328, 1336, 1351, 1356-58, 1380, 1389, 1430, 1441, 1444-45, 1453, 1470, 1500, 1513, 1525. Plaintiffs establish the plausibility of those allegations in detail—showing how Defendants' unlawful acts caused millions of dollars, horrific weapons, advanced technology, and other key resources and benefits to flow to the very terrorists that attacked Plaintiffs. *See supra* pp.14-18. Those allegations are the tip of the iceberg. Defendants actively enabled terrorist agents and fronts to conceal their fundraising—and the full knowledge of Binance's interactions with terrorists "rests in Defendants' sole control." ¶748. "[D]iscovery will show substantially more transactions on the Binance exchange occurring contemporaneously with the attacks in this case—causing even more value to flow through to the FTOs who committed the attacks." *Id*.

That is enough. Contrary to Defendants' suggestion, no court has required plaintiffs to forensically trace dollars through the opaque machinery of terrorist finance and show that specific dollars were used in specific attacks. Instead, courts uniformly recognize that money "is fungible" and terrorists "can hardly be counted on to keep careful bookkeeping records," *Owens v. Republic of Sudan*, 864 F.3d 751, 799 (D.C. Cir. 2017), *vacated and remanded sub nom.*, *Opati v. Republic of Sudan*, 590 U.S. 418 (2020), and so "trac[ing] specific dollars to specific attacks … would be impossible and would make the ATA practically dead letter," *Schansman v. Sberbank of Russia PJSC*, 565 F. Supp. 3d 405, 418-19 (S.D.N.Y. 2021).

Unsurprisingly, the Supreme Court has held that liability does not require "a strict nexus between the alleged assistance and the terrorist act." *Twitter*, 598 U.S. 497. Liability also does not require the defendant to know about or direct support to a particular attack—or even to attacks generally. Instead, those who aid and abet *any* unlawful act "can be held liable for other torts that were 'a foreseeable risk'" of the act they aid and abet. *Id*. at 496. Foreseeability is a question of fact—and Plaintiffs plausibly allege that the attacks that injured them were foreseeable risks of enabling the terrorists' cryptocurrency transactions. *E.g.*, ¶23. Thus, providing "aid to a known terrorist group would justify holding a secondary defendant liable for all of the group's actions or perhaps some definable subset of terrorist acts" when, for example, "the provider of routine services does so in an unusual way or provides such dangerous wares that selling those goods to a terrorist group could constitute aiding and abetting a foreseeable terror attack." *Twitter*, 598 U.S. at 502. Defendants did all of that, and more. As explained in detail *infra*, all of their arguments for dismissal lack merit.

I. This Court Has Personal Jurisdiction Over Binance US

BHL has not challenged personal jurisdiction. But Binance US contests jurisdiction on statutory and constitutional grounds. Neither objection has merit. Regarding statutory jurisdiction,

an ATA case may be instituted "where any plaintiff resides or where any defendant … is served, or has an agent," and process may be served "in any district where the defendant resides, is found, or has an agent." 18 U.S.C. § 2334. "[T]his provision permits the exercise of personal jurisdiction over parties properly served anywhere in the United States." *Zobay v. MTN Grp. Ltd.*, 695 F. Supp. 3d 301, 322 (E.D.N.Y. 2023); *see also Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140, 152 (E.D.N.Y. 2017), *aff'd in part, dismissed in part* 934 F.3d 53 (2d Cir. 2019). Binance US was served in this district: Plaintiffs properly served the company via its Chief Compliance Officer, who resides here, *see* Singh Decl. ¶3, Ex. A; Fed. R. Civ. P. 4(h)(1)(B), and Binance US does not contend that service was insufficient. Moreover, at least one plaintiff resides in this district. Singh Decl. ¶4.

As Binance US acknowledges, the constitutional specific-jurisdiction inquiry in a federal case asks whether a claim arises out of or relates to the defendant's contacts with "the United States as a whole." BAM Mem. 7. Binance US has more than minimum contacts with the United States: It is a U.S. business where U.S. employees serve a U.S. customer base in ostensible compliance with all U.S. laws. ¶31. That is more like maximum contacts than minimum ones.

In addition, Binance US's co-defendants' have substantial U.S. contacts—including the use U.S. customers, partners, and banks (several in New York), to carry out the scheme. ¶¶1549-77. These contacts are attributable to Binance US on two independent theories. *First*, as explained *supra* p.9, Binance US was effectively an alter ego of Binance and Zhao. "It is … well established that the exercise of personal jurisdiction over an alter ego corporation does not offend due process." *S. New England Tel. Co. v. Glob. NAPs Inc.*, 624 F.3d 123, 138 (2d Cir. 2010). And the federal test is satisfied if "it would be unfair under the circumstances not to disregard the corporate form." *Id.* at 139. Binance US asserts that the complaint lacks factual allegations supporting this alter-ego thesis. BAM Mem. 3-4. But the supporting facts are legion. Binance US was indirectly owned and

controlled by Zhao, ¶¶32-34. Zhao and Binance also controlled Binance US's bank accounts, cryptocurrency assets, data, and business transactions. Indeed, two CEOs of Binance US stated that the company was controlled not by them, but by Binance and Zhao.

More broadly, "Binance US's *raison d'etre* was to serve as an instrument that Binance and Zhao could (and did) use to influence the conduct of U.S. government officials," ¶1579—specifically, to advance "their scheme to, among other objectives, forestall regulation of Binance's illegal activities and deflect the attention of U.S. lawmakers, regulators, and law enforcement agencies away from Binance and its illegal activities," ¶1580. Binance US also acted as Binance's recruiting ground for high-volume U.S. customers, which Binance and Zhao migrated to Binance.com. Binance US thus helped Binance "surreptitiously (and illegally) retain its substantial base of U.S. users (particularly those with the greatest transaction volumes and trading frequency) while avoiding the obligation to bring its operations into compliance with U.S. laws and regulations applicable to money service businesses with U.S. operations—including AML/CFT and KYC requirements, other FinCEN regulations, sanctions laws, and the Bank Secrecy Act, to name a few." ¶31; *see also* ¶¶683-85. Binance and Zhao thus controlled all relevant features of Binance US's operations, such that "actions performed by [Binance entities, including Binance US] are legally attributable to Zhao and Binance and vice versa." ¶34. Nothing in Binance US's declaration contradicts these allegations—which are sufficient to establish Binance US as an alter ego of its co-defendants.[3]

[3] Even if the assertions in the declaration contradicted Plaintiffs' allegations, the Court would be required to accept the allegations at this stage of the proceedings. *See, e.g.*, *Schwab Short-Term Bond Mkt. Fund v. Lloyds Banking Grp. PLC*, 22 F.4th 103, 123-24 (2d Cir. 2021); *Dorchester Fin. Sec., Inc. v. Banco BRJ, S.A.*, 722 F.3d 81, 86 (2d Cir. 2013) (per curiam).

Second, Binance US's co-defendants' contacts are attributable to Binance US under the theory of conspiracy jurisdiction—which arises when the defendant participated in a conspiracy, and a co-conspirator's overt acts in furtherance of the conspiracy had sufficient contacts with the forum. *See In re Platinum & Palladium Antitrust Litig.*, 61 F.4th 242, 270 (2d Cir. 2023); *Charles Schwab Corp. v. Bank of Am. Corp.*, 883 F.3d 68, 86 (2d Cir. 2018). Plaintiffs allege that Binance US conspired with Zhao and BHL—and that BHL directed substantial activities at New York and the United States, including transferring cryptocurrency between millions of U.S. customers and prohibited foreign users, ¶¶1551-52, 1566-73, and using American partners (including New York companies and banks) to facilitate its scheme, ¶¶1553-64, 1574. These constitutional contacts also provide an alternative basis for statutory jurisdiction under the New York long arm statute. *See Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 171 (2d Cir. 2013) ("[T]he selection and repeated use of" New York businesses "as an instrument for accomplishing the alleged wrongs for which the plaintiffs seek redress" supports personal jurisdiction).

Binance US contends that Plaintiffs' claims do not arise out of or relate to its in-forum contacts. BAM Mem. 8-9. Plaintiffs need not show that BAM's in-forum conduct *caused* the plaintiff's injuries. *See Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 592 U.S. 351, 362 (2021). Instead, it suffices to show that the plaintiff's claim "relates to" those contacts. *See id.* If the court correctly attributes all of Defendants' contacts to Binance, then Plaintiffs' claims obviously relate to those contacts because the contacts were part of Binance's scheme to engage in terrorist finance. Even if the Court does not impute its' co-defendants' contacts to Binance, Plaintiffs' claims relate to Binance US's in-forum activities because its in-forum role as a lightning rod for U.S. regulatory attention (distracting away from Binance.com) was a key element of the scheme that allowed Binance and Zhao to serve FTOs and the Terrorist Sponsors. Binance's service of those terrorist

entities, in turn, gives rise to Plaintiffs' claims. Thus, even though Binance US's conduct is one step removed from actually serving terrorists, it has a sufficient relationship to Plaintiffs' claims to subject Binance US to this Court's jurisdiction consistent with due process.

Independently, Binance US is subject to "tag" jurisdiction because its Chief Compliance Officer was served in the district. *See Burnham v. Sup. Ct.*, 495 U.S. 604, 618-19 (1990) (explaining historical and constitutional basis for tag jurisdiction, *i.e.*, that "jurisdiction based on physical presence alone constitutes due process because it is one of the continuing traditions of our legal system"). The Second Circuit has held that when a partner was served with a subpoena in the forum, the court had jurisdiction over the entire foreign partnership and could compel it to respond. *See First Am. Corp. v. Price Waterhouse LLP*, 154 F.3d 16, 20 (2d Cir. 1998). The same logic applies to corporations and their officers. Although some courts have rejected tag jurisdiction for corporations, the better view is that it is consistent with due process principles—and in any event, Second Circuit precedent permits it. *See generally* Cody J. Jacobs, *If Corporations Are People, Why Can't They Play Tag?*, 46 N.M. L. Rev. 1 (2016) (describing the venerable history of corporate tag jurisdiction and explaining why due process principles favor it).

II. Defendants' Rule 8 Argument Is Meritless

Dismissal is not warranted for violation of Rule 8's "short and plain" statement rule. Dismissal on this ground requires the complaint to be "so confused, ambiguous, vague, or otherwise unintelligible that its true substance, if any, is well disguised." *Salahuddin v. Cuomo*, 861 F.2d 40, 42 (2d Cir. 1988); *Smith v. Fischer*, 2016 WL 3004670, at *3-4 (W.D.N.Y. May 23, 2016) (holding that dismissal is warranted only where "the complaint is so rambling that it is incomprehensible"). Under this rule, "long and involved complaints do not *per se* fail to pass the test of sufficiency under Rule 8." *Burke v. Dowling*, 944 F. Supp. 1036, 1049 (E.D.N.Y. 1995) (quotation omitted). Instead, dismissal should be denied if "courts and adverse parties can

understand a claim and frame a response to it." *Id.*; *see also Wynder v. McMahon*, 360 F.3d 73, 80 (2d Cir. 2004); *Harnage v. Lightner*, 916 F.3d 138, 142 (2d Cir. 2019).

Moreover, "[b]revity must be calibrated to the number of claims and also to their character, since some require more explanation than others to establish their plausibility." *Kadamovas v. Stevens*, 706 F.3d 843, 844 (7th Cir. 2013). Consistent with this admonition, courts have permitted ATA complaints similar to this one. *See Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204, 213 (D.C. Cir. 2022) (sustaining complaint that was "588 pages long" and "provide[d] context and spell[ed] out connections relevant to the extraordinary events it describes … with reference to hundreds of identified sources"), *cert. granted, judgment vacated*, 144 S. Ct. 2675 (2024); *Bartlett v. Société Générale de Banque Au Liban SAL*, 2020 WL 7089448, at *1 (E.D.N.Y. Nov. 25, 2020) (allowing 5,695 paragraph complaint spanning 788 pages). This is not the only context in which robust complaints have survived motions to dismiss. *See, e.g.*, *In re Glob. Crossing, Ltd. Sec. Litig.*, 313 F. Supp. 2d 189, 212 (S.D.N.Y. 2003) (refusing to dismiss 326-page complaint alleging multiple claims rooted in a complex fraud).

Plaintiffs' complaint, although comprehensive and detailed, is organized according to subject headings explaining what Defendants did wrong, and how their misconduct enabled the attacks that injured Plaintiffs. Accordingly, the complaint provides adequate notice to Defendants of the nature of the claims against them, and enables them to prepare a response (which they have done). Despite its length, it does not violate the Second Circuit's forgiving Rule 8 standard.

Defendants do not seriously argue otherwise. Instead, their Rule 8 argument asserts, without much substantiation, that many of Plaintiffs' allegations are not sufficiently related to their claims. BHL Mem. 10. Thus, Defendants argue that Iran's historic pattern of sponsoring terrorism is not relevant to Plaintiffs' claims. But "[t]errorism scholars have confirmed that historical context

is vital to understanding Iran-sponsored terrorism during the 2000s and 2010s." ¶66. The history—from authoritative, public sources—serves two functions: (1) it "confirm[s] the plausibility of Plaintiffs' allegations"; and (2) it "alerted Defendants as to the nature of their counterparties and/or the ultimate beneficial owners of the transactions Defendants facilitated." *Id*.

Defendants also try to nitpick allegations relating to a handful of attacks. For example, they contend that the complaint does not sufficiently link Defendants' misconduct to the Pensacola attack by al-Qaeda in the Arabian Peninsula (AQAP). BHL Mem. 11. Putting aside that this is not a Rule 8 objection at all, it is based on a mischaracterization of the law and of Plaintiffs' allegations. The law does not require Plaintiffs to trace the resources Defendants provided through to the specific attack; it is enough to establish that Defendants' conduct was unlawful and the attacks were a foreseeable risk of that conduct. As to the allegations, Plaintiffs do not merely vaguely allege that Defendants' conduct caused profits to flow to Iranian groups that, in turn, provided communications technology to AQAP. *Contra* BHL Mem. 11. Instead, Plaintiffs recount the history by which Iran's Terrorist Sponsors helped establish AQAP as a branch of al-Qaeda and cultivated their relationship with it by providing logistics, technical, and financial support (including but not limited to sophisticated communications technology that could only come from the Terrorist Sponsors). ¶¶142, 177, 1423, 1432-40, 1458. Plaintiffs discuss how the Terrorist Sponsors gleaned money from cryptocurrency transactions enabled by Binance and used it to finance attacks by AQAP (among others). ¶¶1452-56. Plaintiffs identify Iran Electronics Industries (IEI), another relevant IRGC front, as a key provider of weapons to AQAP. ¶¶437-38, 997-1000. Plaintiffs also provide an example of AQAP using cryptocurrency to finance attacks around the world. ¶604. And they allege that the attack in question "was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support," as well

as "the Terrorist Sponsors' use of, and provision to" AQAP "of, communications, telecommunications, or computing technologies" manufactured by the Terrorist Sponsors and their fronts, including IEI. ¶¶2761-63. Plaintiffs thus allege that Defendants' misconduct allowed the Terrorist Sponsors, and by extension AQAP, to access specific resources that enabled the attack.

Defendants also challenge the connection between their conduct and attacks on three bases in Iraq. BHL Mem. 11. But again, their protests are weak. For example, the description of the January 8, 2020 attack on Al Asad Air Base explains that it was committed by the IRGC, together with a joint cell comprising operatives from Hezbollah and Kataib Hezbollah, all of which were funded, armed, and logistically supported by the Terrorist Sponsors. ¶1675. The complaint names specific leaders involved in the attack, ¶¶1676-77, who were also beneficiaries of Defendants' misconduct, ¶¶485-86, 937-42, 1179, 1192, 1221-23, 1227, 1236, 1239-42, 1250-53. It also describes, in detail, the missiles, rockets, UAVs, other weapons, and intelligence resources the attackers used, ¶¶1675, 1683-88, which were all technologies that Defendants' misconduct helped fund, ¶¶1019, 1024-83, 1103-48. And it explains why the Terrorist Sponsors' financial resources were essential to carrying out the attack. ¶¶1681-82. Again, the link between Defendants' misconduct and the attack is clear: Defendants—through their unlawful evasion of Iran-facing counterterrorism sanctions—provided the resources necessary for the Terrorist Sponsors and the IRGC to plan the attack, and for the IRGC, Hezbollah, and Kataib Hezbollah to commit it.

Even if the Court perceives a Rule 8 problem, amendment can cure it. "[I]t will generally be an abuse of discretion to deny leave to amend when dismissing a nonfrivolous original complaint on the sole ground that it does not constitute the short and plain statement required by Rule 8." *Blakely v. Wells*, 209 F. App'x 18, 20 (2d Cir. 2006) (quoting *Salahuddin*, 861 F.2d at 42). Defendants argue that dismissal with prejudice is permitted when a complaint has already been

amended—but that applies only when amendments made in response to a Rule 8 argument failed to cure the defect. Here, Defendants never raised a Rule 8 challenge to the original complaint. *See* ECF 22. Accordingly, the Amended Complaint "should be treated as the original complaint" for Rule 8 purposes, and dismissal with prejudice would be an abuse of discretion. *Gatling-Brooks v. Liberty Mut. Ins. Co.*, 2024 WL 5186527, at *3 (S.D.N.Y. Dec. 20, 2024).

III. Plaintiffs State An Aiding And Abetting Claim

To plead a JASTA aiding and abetting claim, a plaintiff must allege that the defendant (1) was "generally aware of his role as part of an overall illegal or tortious activity at the time that he provide[d] the assistance"; and (2) "knowingly and substantially assist[ed] the principal violation." *Twitter*, 598 U.S. at 486. Plaintiffs have pled each element.

A. Plaintiffs allege "general awareness."

Binance was (at least) "generally aware of [its] role as part of an overall illegal or tortious activity at the time that [it] provide[d] the assistance." *Honickman v. BLOM Bank SAL*, 6 F.4th 487, 494 (2d Cir. 2021). This requirement "is not an exacting one." *Raanan*, 2025 WL 605594, at *19. A defendant need not be "generally aware of its role in the specific act that caused the plaintiff's injury; instead, it must be generally aware of its role in an overall illegal activity from which the act that caused the plaintiff's injury was *foreseeable*." *Honickman*, 6 F.4th at 496. In contrast with actual knowledge, general awareness connotes "something less than full, or fully focused, recognition." *Kaplan*, 999 F.3d at 863. At the pleading stage, awareness of a fact can be established by identifying public sources stating it; but it is not necessary "to allege that [the defendant] knew or should have known of the public sources at the pleading stage. Such a requirement at this juncture would be too exacting." *Honickman*, 6 F.4th at 501. Controlling precedents also reject Binance's assertion that general awareness requires showing that "BHL intended to further any FTO's terrorist activities," BHL Mem. 23. *See Kaplan,* 999 F.3d at 858

(rejecting argument that "a JASTA aiding-and-abetting plaintiff must plead and prove the defendant's intent to participate in international terrorism"); *Twitter*, 598 U.S. at 497, 504 (holding this element satisfied by allegations "that defendants knew they were playing some sort of role in ISIS's enterprise," despite an "undisputed lack of intent to support ISIS").

Binance was more than "generally aware" of its role in "overall illegal" activities. Illegal activities were key to its "business strategy," which was "to operate [an] illegal cryptocurrency exchange in the United States … while willfully violating U.S. AML/CFT rules and regulations, U.S. sanctions, and U.S. reporting requirements," ¶731—conduct to which Binance pled guilty. Zhao "prioritized [Binance's] growth and profits over compliance with U.S. law," telling employees it was "'better to ask for forgiveness than permission.'" ¶29, while the company's compliance personnel actively worried about "land[ing] in jail" because they were "teaching ppl how to circumvent sanctions," knowing that "Binance's users were 'here for crime,'" ¶643. Indeed, it is breathtaking that a company that admitted these violations and paid a $4 billion penalty can now argue that it was not even generally aware that it did anything unlawful.

Binance's claim that "[t]he Complaint does not allege that BHL was warned that specific Binance customers were engaged in terrorism, nor that certain of the generalized warnings—such as those by NGOs and terrorism scholars—were even known to BHL," BHL Mem. 22-23, is flatly wrong. For example, Plaintiffs expressly allege that "a third-party service provider flagged [Binance] accounts associated with ISIS and Hamas"—accounts that Binance nevertheless kept open. ¶1259. Quoting Binance's *own statements*, Plaintiffs further allege that Binance implemented sophisticated tools to identify the nature of its customers and screen their transactions. ¶¶662-72; *see* ¶657. As to more general warnings, Plaintiffs allege that "Binance regularly monitored (but willfully disregarded) warnings from the U.S. government, international

community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by FTOs." ¶538; *see also* ¶¶539, 566-67, 572, 585-86, 595-96, 713-14, 1481-83, 1488 (additional allegations that Binance either knew of public warnings or received direct warnings from authoritative sources). The court found similar allegations sufficient in *Raanan*. *See* 2025 WL 605594, at *20. In any event, Defendants flagrantly misstate the law. The analysis they cite—drawn from the district court's decision in *Honickman*—was expressly rejected on appeal, when the Second Circuit held that it would be "too exacting" to require plaintiffs "to allege that [the defendant] knew or should have known of the public sources at the pleading stage." *Honickman*, 6 F.4th at 501.[4]

Binance US's argument that "knowledge of Iran's status as a state sponsor of terrorism" is insufficient to establish general awareness is similarly flawed. BAM Mem. 12. The quoted language appears in *O'Sullivan v. Deutsche Bank AG*, 2019 WL 1409446, at *10 (S.D.N.Y. Mar. 28, 2019)—a case that is neither controlling nor persuasive. *First*, the decision relied on the wrong legal rule, positing that plaintiffs had to show that the defendants were aware that they were playing a role in terrorist attacks specifically. The Second Circuit rejected that rule, clarifying that general awareness can be of any "overall illegal activity"—not only terrorist attacks. *Honickman*, 6 F.4th at 496. *Second*, the allegations in *O'Sullivan* about Iran's systematic role in FTO terrorism were not as robust as the allegations here—and to the extent they are comparable, *O'Sullivan* wrongly

[4] Binance US contends that Plaintiffs' allegations are internally contradictory because Binance could not simultaneously have had deliberately anemic AML controls, while also alleging that Binance received information about its customers from blockchain analysis firms. BAM Mem. 13. But there is no contradiction. Plaintiffs allege (and Binance has admitted) that it had deliberately anemic AML controls for several years, pursuant to which it onboarded customers and facilitated their transactions without collecting essential information, and without ever reporting suspicious transactions. Nevertheless, Binance advertised that it contracted with sophisticated analysis firms, and accordingly received key information about at least some of its customers showing their terrorist affiliations. From there, Plaintiffs allege that Binance *either* ingested that information (and therefore knew it), *or* willfully blinded itself to the information. Either way, Plaintiffs state a claim.

disregarded them. In addition to the general rule that courts *must* credit well-pleaded allegations, Congress and the Executive Branch—the political branches charged with protecting our national security—have unequivocally and emphatically explained that providing support to the Terrorist Sponsors is both unlawful and dangerous, and specifically places American lives at risk. *E.g.*, ¶¶164, 178, 213, 224-243, 314, 356, 404-09, 568-71, 609, 676-78, 824-30, 832-33, 967, 1089-90, 1182-85, 1287-88, 1314-15. Courts have no license to second-guess those determinations. *Cf. Holder v. Humanitarian L. Project*, 561 U.S. 1, 33-34 (2010) (explaining that when litigation "implicates sensitive and weighty interests of national security and foreign affairs," the "evaluation of facts by the Executive, like Congress's assessment, is entitled to deference"); *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 871-72 (2d Cir. 2008) (explaining that courts should defer to the executive regarding national security matters, including terrorism).

Binance US's reliance on *Siegel v. HSBC North America Holdings, Inc.*, 933 F.3d 217 (2d Cir. 2019), is similarly unpersuasive. As the Second Circuit explained in *Kaplan*, the facts of *Siegel* were a far cry from the facts here. Thus, the defendant in *Siegel*, "after learning of reports that [its customer] had customers who were terrorists, terminated its relationship with [the customer] nearly a year before the relevant terrorist attacks occurred," making it implausible that the bank was aware of a role in terrorism. *Kaplan*, 999 F.3d at 862. Moreover, the defendant's customer in *Siegel* "was another bank, ARB, Saudi Arabia's largest bank with worldwide operations." *Id*. In *Kaplan*, the Second Circuit relied on these facts to distinguish *Siegel* while upholding liability for a bank that did business with "persons and entities who were in fact integral parts of Hizbollah," and violated "banking regulations" on those customers' behalf, "allowing them … to circumvent existing sanctions on Hizbollah as a designated FTO." *Id*. This case far more closely resembles *Kaplan*: Binance's customers were members of FTOs, as well as fronts for the IRGC and other Terrorist

Sponsors. *E.g.*, ¶¶17, 502. Binance's services to those customers violated many laws. *E.g.*, ¶¶503-07, 631. And when confronted with evidence that it was serving terrorist customers, Binance persisted. *E.g.*, ¶¶632-43. Tellingly, Binance US repeatedly cites both the district and circuit court opinions in *Siegel*, but never even mentions *Kaplan*.

B. Plaintiffs allege "knowing and substantial assistance."

Binance also provided "knowing and substantial" assistance to the perpetrators of the attacks. *Twitter* clarified that this element aims "to capture conscious and culpable conduct," 598 U.S. at 504, and calls for courts to balance "the nature and amount of assistance" with "the defendant's scienter," *id.* at 492-93. That is, "less substantial assistance require[s] more scienter," and "vice versa." *Id*. at 492. *Twitter* also holds that aiding-abetting liability requires some "nexus" between the aid and the terrorist act. *Id*. at 497. However, "[a]s *Halberstam* makes clear, people who aid and abet a tort can be held liable for other torts that were 'a foreseeable risk' of the intended tort," such that while "a close nexus between the assistance and the tort might help establish" aiding and abetting, "even more remote support can still constitute aiding and abetting in the right case." *Id.* at 496.

1. Plaintiffs allege that Binance culpably engaged in active misconduct.

Plaintiffs allege more than necessary to satisfy the common law standard for knowing and substantial assistance by alleging *both* highly culpable scienter *and* that Defendants provided massive amounts of support to violent terrorists.

Binance argues that it did not engage in conscious, voluntary, and culpable conduct because all it allegedly did was fail to stop bad actors from using its platform—similar to the allegations that failed in *Twitter*. But as explained *supra* pp.4-9, Binance's misconduct was active, not passive. Contrary to Binance's mischaracterization of the complaint, Plaintiffs allege that Binance actively invited and facilitated terrorist finance. Thus, Binance deliberately avoided implementing anti-

terrorism controls; sabotaged the controls it did implement by making them weak and coaching criminal users to avoid them; consistently lied to regulators and other third parties about its practices; and took other active steps to cater to terrorist users, including obstructing law enforcement investigations. *Cf. Raanan*, 2025 WL 605594, at *21 ("[C]onstrued in the light most favorable to the plaintiffs, the Amended Complaint alleges more than mere 'passive nonfeasance'" because "plaintiffs claim that the defendants took affirmative actions to enable terrorist groups to transact on the Binance platform.").

This renders *Twitter* inapposite. In *Twitter*, most of the allegations rested on "mere passive nonfeasance," *i.e.*, failure to stop terrorists from using social media platforms—which had "no duty … to terminate customers after discovering that the customers were using the service for illicit ends." 598 U.S. at 500-01. As *Twitter* explained, where a defendant is accused of mere "passive nonfeasance" in the absence of any legal duty to act, liability requires a strong showing of scienter and substantiality because the law is "leery" of imposing liability for inaction. *Id*. at 500. In contrast, where the defendant engaged in active misconduct—which is "the traditional predicate for liability in tort"—a lesser showing suffices. *Zobay*, 695 F. Supp. 3d at 347 (citing *Twitter*, 598 U.S. at 500); *see also Bonacasa v. Standard Chartered PLC*, 2023 WL 7110774, at *10 n.13 (S.D.N.Y. Oct. 27, 2023).

Twitter itself supports this distinction. The passive allegations in *Twitter* failed for want of "a strong showing of assistance and scienter." 598 U.S. at 500. But the Court analyzed separately allegations that Google had actively "shared advertising revenue with ISIS." *Id*. at 505. With respect to those active-support allegations, the Court did not require any heightened showing—but instead held that the complaint failed to state a claim because it "allege[d] nothing" about the quantity of support—which could have been "only $50." *Id*. The Court's analysis *strongly* implies

that if the plaintiffs had alleged that Google provided a substantial amount of active support to ISIS, the result would have been different. That is what Binance did here by providing access to vast sums of money—as well as the eight other benefits discussed *supra* p.15. It is also what Binance did by coaching customers on how to evade its own KYC protocols as well as international sanctions; by covering for its criminal customers instead of reporting them; and by lying to the public and governments about its compliance practices. *See supra* pp.4-9.

Binance's reliance on its supposed passivity also fails because Binance was legally required to take affirmative measures to identify and block terrorists attempting to use its exchange, and to report those transactions. *E.g.*, ¶506, 607-18. The company deliberately evaded those duties to obtain commercial advantage. *E.g.,* ¶¶6, 29, 500, 509-12, 646, 681-84, 711. In light of its duties, even the actions that Binance characterizes as "passive" constituted *criminal* misconduct on a massive scale. Such allegations are "a crucial point of departure between [*Twitter*] and this case." *Zobay*, 695 F. Supp. 3d at 346; *see Twitter*, 598 U.S. at 489 (recognizing that "inaction can be culpable in the face of some independent duty to act"); *cf. Raanan*, 2025 WL 605594, at *21 (holding that Binance "had an independent duty to act that was not present in *Twitter*," including obligations "to implement robust anti-money laundering programs, perform due diligence on customers, and file SARs with regulators flagging suspected illicit activity, all to prevent terrorists from accessing the United States financial system through the Binance exchange").

The Second Circuit's aiding-abetting jurisprudence makes the same distinction, holding that "[s]ubstantial assistance occurs when a defendant affirmatively assists, helps conceal or fails to act when required to do so." *SPV Osus Ltd. v. UBS AG*, 882 F.3d 333, 345 (2d Cir. 2018). Common-law cases that *Twitter* cited approvingly likewise hold that when a defendant has a duty to act, a lesser showing of culpability suffices. *See, e.g.*, *Camp*, 948 F.2d at 459 (relying on Second

Circuit precedent to hold that "[r]ecklessness satisfies the knowledge requirement where the defendant owes a duty of disclosure to the plaintiff"); *Woods v. Barnett Bank of Ft. Lauderdale*, 765 F.2d 1004, 1010 (11th Cir. 1985) (holding that "liability could be imposed upon an aider and abettor who is under a duty to disclose if he acts with a lesser degree of scienter").[5]

Independently, the bar for finding that Binance acted culpably is low because, as explained *supra* p.20, Binance's actions were not routine, but instead represented extraordinary departures from ordinary business practices, even in the crypto industry. *Twitter* recognized that "where the provider of routine services does so in an unusual way," that could "constitute aiding and abetting a foreseeable terror attack." 598 U.S. at 502. The Court referenced common-law cases embodying a similar rule. For example, in *Camp*, the court explained that the level of knowledge "necessary for liability remains flexible and must be decided on a case-by-case basis." 948 F.2d at 459 (cited in *Twitter*, 598 U.S. at 491-92). Thus, "[a] party who engage[d] in atypical business transactions … may be found liable as an aider and abettor with *a minimal showing of knowledge*." *Id.* (emphasis added); *see also Woods*, 765 F.2d at 1009-10, 1012 (cited in *Twitter*, 598 U.S. at 492) (holding that when a "method or transaction is atypical or lacks business justification, it may be possible to infer the knowledge necessary for aiding and abetting liability," and holding that when bank employees wrote a favorable reference for a customer without first conducting diligence, the bank was properly held liable for the customer's fraud). Under these precedents, which are part of

[5] BHL says nothing about its affirmative duties. Binance US argues in a single sentence that the duty to have AML and KYC policies is not enough to create a duty, citing a fraud case, *Rosner v. Bank of China*, 528 F. Supp. 2d 419, 427 (S.D.N.Y. 2007). BAM Mem. 16. But *Rosner* merely held that legal violations, without more, do not constitute substantial assistance. It said nothing about whether those laws create duties that influence the aiding-and-abetting calculus. In any event, this case is different because the legal violations were the mechanism by which Binance provided substantial assistance to FTOs and the Terrorist Sponsors. *Cf. Raanan*, 2025 WL 605594, at *21 (holding that the same duties support liability under *Twitter*).

the common law framework that *Twitter* endorsed, the Court can infer culpability from the unusual nature of Binance's transactions alone.

On the other hand, even if Binance's misconduct were passive, that would not foreclose liability; it would only require a stronger showing of scienter and assistance. Plaintiffs have made that showing by alleging that Binance deliberately failed to establish and enforce anti-terrorism controls *specifically* to assist its criminal customers in their illicit efforts—which in turn allowed those customers to access at least millions of dollars. *See supra* pp.10-13.

Finally, to the extent Binance claims that it did not actually know that it was assisting terrorists—and Plaintiffs have alleged incidents in which it did, *e.g.*, ¶¶631, 636-38, 767, 1263, 1266, 1393, 1489—it's because Binance was willfully blind to its customers' identities, despite its legal obligation to find out. *See supra* p.13. Willful blindness to a known risk "is as culpable as actual knowledge." *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 766 (2011); *Unicolors, Inc. v. H&M Hennes & Mauritz, L. P.*, 595 U.S. 178, 187 (2022) ("[I]n civil cases … willful blindness may support a finding of actual knowledge."). Tellingly, Defendants' motions do not address the willful blindness allegations *at all*.

2. Plaintiffs allege the necessary "nexus" between Binance's misconduct and the terrorist attacks.

Twitter requires some connection between the Defendants' assistance and the attacks that injured Plaintiffs, but recognizes that a "strict nexus" is ***not*** required and that "even more remote support can still constitute aiding and abetting." 598 U.S. at 503. Where, as here, Plaintiffs "allege affirmative misfeasance, rather than merely passive nonfeasance, *Twitter* … does not require as close a nexus between [the defendant's] actions and the attacks." *Bonacasa*, 2023 WL 7110774, at *10 (citing *Twitter*, 598 U.S. at 496-97, 500-02, 505). Plaintiffs allege three forms of nexus, each of which is independently sufficient under *Twitter*: (1) Defendants assisted the attacks that injured

Plaintiffs; (2) Defendants assisted unlawful acts including terrorist finance and the evasion of anti-terrorism sanctions on the Terrorist Sponsors, and that the attacks that injured Plaintiffs were a foreseeable risk of the acts Defendants assisted; and (3) Defendants provided such pervasive and systemic assistance to the terrorists' enterprise that they are properly liable for all of the attacks at issue here.

First, Plaintiffs allege that Binance assisted the attacks that injured them. Plaintiffs explain how Binance enabled transactions that caused millions of dollars, deadly weapons, and advanced technology to flow to the terrorists who planned and committed the attacks. *See supra* pp.14-18, 21-22, 29-30. As explained *supra*, this included directly enabling FTOs to transact in cryptocurrencies, as well as enabling the Terrorist Sponsors to plan and coordinate attacks, as well as raise and move money and other resources to their terrorist proxies. Those resources enabled the terrorist cells to attack Americans, including Plaintiffs. These allegations are specific, describing terror cells and in many instances specific terrorists who benefited from Binance's assistance, and used those benefits to plan or commit the attacks that injured Plaintiffs. *Cf. Zobay*, 695 F. Supp. 3d at 346 (upholding JASTA liability when defendant's actions caused money and technology to flow to the IRGC and on to its terrorist proxies).

To be sure, Binance may not have specifically intended to assist any particular attack, or known about them in advance—but as *Twitter* explains, such knowledge is not necessary. 598 U.S. at 495. It is enough that Binance provided illicit cryptocurrency transfer services to terrorist groups known to use cryptocurrency to fund *attacks*, rather than other activities, *e.g.*, ¶¶570, 592, 604, 1270-71, 1275, during the relevant time period. By doing so, Binance knowingly and substantially participated in the causal chain leading to terrorist violence—including the attacks that injured Plaintiffs.

Second, "*Twitter* continues to recognize that, where a defendant consciously and culpably aided wrongful acts, liability may attach to acts of terrorism that are foreseeable risks of those acts." *Bonacasa*, 2023 WL 7110774, at *8; *Twitter*, 598 U.S. at 487 (recognizing that, in *Halberstam*, the defendant "Hamilton substantially helped Welch commit personal property crimes and was liable for Halberstam's death, which was a foreseeable result of such crimes"). Plaintiffs have alleged in detail why the attacks were a foreseeable risk of Binance's culpable participation in sanctions evasion and terrorist finance. Copious government and third-party warnings explained that providing illicit cryptocurrency services to terrorist organizations and their supporters was tantamount to subsidizing the murder of Americans. *See supra* pp.14-18. Not only was Binance the world's largest cryptocurrency exchange in this period, but it was also "the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements," ¶1276—making it by far the mostly likely exchange for the terrorists to use in raising funds for the attacks on Plaintiffs. This is all the "nexus" that *Twitter* requires. 598 U.S. at 496; *see Zobay*, 695 F. Supp. 3d at 340 (holding that plaintiffs satisfied foreseeability nexus by alleging that the defendant partnered with IRGC fronts that acquired military and other prohibited technology and supplied Hezbollah and other terrorist proxies with weapons, training, and funding); *Bonacasa*, 2023 WL 7110774, at *11 (holding foreseeability nexus satisfied when defendant bank made commercial loans to fertilizer company known to facilitate the production of fertilizer that was used in terrorist explosives); *King*, 2023 WL 8355359, at *3 (holding that bank that provided financial services to terrorists in unusual ways could be liable for foreseeable terrorist attacks). Neither defendant discusses foreseeability at all in their motions.

Third, where a defendant's assistance to a terrorist group is "pervasive, systemic, and culpable," it may be held liable for *all* that group's attacks, "or perhaps some definable subset."

Twitter, 598 U.S. at 501-02. As examples, *Twitter* noted that a "provider of routine services" might do "so in an unusual way," or might "provide[] such dangerous wares that selling those goods to a terrorist group could constitute aiding and abetting a foreseeable terror attack." *Id*. at 502. That, of course, is exactly what Binance did when it actively and illegally enabled billions of dollars in cryptocurrency transactions for FTOs and the Terrorist Sponsors. *See, e.g.*, ¶14 (explaining that "cryptocurrency posed uniquely dangerous terrorist financing risks"); *see also* ¶¶20, 537, 588, 716 (similar). *Cf. Raanan*, 2025 WL 605594, at *22 ("In short, the plaintiffs have alleged that the defendants provided services that might otherwise be considered routine—cryptocurrency transaction services—in an unusual way—designed to evade government detection and regulation…. Binance, in providing financial services that intentionally circumvented anti-terrorist-financing regulations, offered such dangerous wares that selling those goods could constitute aiding and abetting a foreseeable terrorist attack.").

Twitter also held that *Halberstam*—where the defendant assisted the principal tortfeasor by laundering the spoils of his burglaries—provides a "useful" illustration of systemic assistance. 598 U.S. at 496. Here, Binance knowingly helped murderous terrorists launder and access "hundreds of millions of U.S. dollars" over a six-year period, ¶¶501-02, including the proceeds of myriad unlawful activities including sanctions evasion, hostage-taking, ransomware attacks, drug trafficking, and extortion rackets, *e.g.*, ¶¶706, 715, 720-21, 728, 1483, 1526-28. This was enough money to fund the attacks at issue here hundreds of times over. *E.g.*, ¶¶739-46. Binance thus engaged in exactly the kind of "pervasive, systemic, and culpable" assistance for which *Twitter* authorizes liability for all the terrorists' attacks. *See Zobay*, 695 F. Supp. 3d at 347 (defendant's "millions of dollars in funding" and other support to the IRGC "plausibly assist[ed] each and every IRGC-led terrorist attack").

Binance's response—that it is not enough to aid a wrongdoer's acts in general (BHL Mem. 20)—simply ignores how the complaint draws the connections between the money and financial services that Binance provided, on the one hand, and the attacks that injured Plaintiffs, on the other. Binance also ignores the role that foreseeability plays in defining the scope of liability: By engaging in clearly unlawful acts (*i.e.*, terrorist financing and money laundering), Binance took on liability for foreseeable resulting torts—including acts of terrorism by the people it assisted. *See Honickman*, 6 F.4th at 496-97 & n.10 (describing foreseeability as "central" in "establishing the extent of liability under an aiding-and-abetting theory").

Binance's next argument—that JASTA liability cannot apply to assistance to entities "with connections" to terrorists, rather than the terrorists themselves—is based entirely on a passage from a pre-*Twitter* district court decision addressing primary liability. BHL Mem. 20-21 (discussing *O'Sullivan*, 2019 WL 1409446, at *7-8). JASTA by its terms is aimed at both "direct[] and indirect[]" support for terrorists, JASTA § 2(a)(6), and every secondary liability decision to reach the issue has allowed claims involving assistance through intermediaries. *See Kaplan*, 999 F.3d at 855-56; *Zobay*, 695 F. Supp. 3d at 347-48; *Bonacasa*, 2023 WL 7110774, at *8-9; *King*, 2023 WL 8355359, at *3. The allegations here meticulously explain how assistance to the Terrorist Sponsors flowed through to the FTOs that committed the attacks—which is enough for liability under JASTA. Otherwise, liability for terrorist finance would be eviscerated as long as the terrorists were smart enough to "launder donations through a chain of intermediate organizations." *Boim v. Holy Land Found. for Relief & Dev.*, 549 F.3d 685, 702 (7th Cir. 2008) (en banc).

In any event, Plaintiffs allege that Binance frequently assisted terrorists themselves. *E.g.*, ¶¶13, 17, 502. One example is the Hezbollah terrorist, Tawfiq Muhammad Sa'id al-Law, who "moved over $11.9 million in 130 different cryptocurrency transfers through the Binance exchange

over the course of 2023," ¶1153, with money flowing to Hezbollah officials and Houthi terrorists, ¶¶1154-55. Even after Israel sanctioned al-Law and identified his and his associates' wallets on an anti-terrorism sanctions list, Binance continued to allow 19 wallets associated with al-Law to continue to transact *over $53 million* in value. ¶1158. That is but one example.

3. The *Halberstam* factors favor liability.

The six factors in *Halberstam* "capture the essence of aiding and abetting." *Twitter*, 598 U.S. at 504. They are variables, *i.e.*, "a means to determine whether a defendant's participation in another's wrongdoing is sufficiently significant and culpable to impose aiding and abetting liability." *Bonacasa*, 2023 WL 7110774, at *10. Plaintiffs' allegations amply support liability.

Nature of the Act: "[T]he nature of the act involved dictates what aid might matter, *i.e.*, be substantial." *Halberstam*, 705 F.2d at 484. Considering this factor, "a court might a court might also apply a proportionality test to particularly bad or opprobrious acts, *i.e.*, a defendant's responsibility for the same amount of assistance increases with the blameworthiness of the tortious act or the seriousness of the foreseeable consequences." *Id.* at 484 n.13. "Financial support is indisputably important to the operation of a terrorist organization." *Zobay*, 695 F. Supp. 3d at 349; *see also Bonacasa*, 2023 WL 7110774, at *10; *King v. Habib Bank Ltd.*, 2022 WL 4537849, at *9 (S.D.N.Y. Sept. 28, 2022). Illegal financial support, provided in defiance of mandatory anti-terrorism controls, is even more valuable. *See* ¶¶719-47 (documenting the key role that access to money played in enabling violence by the specific groups at issue here). And of course, such acts are particularly grave—supporting a strong inference of culpability.

Amount of Assistance: Plaintiffs allege that Binance "allow[ed] the IRGC, Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS to make, receive, and move ***hundreds of millions*** of U.S. dollars in violation of anti-terrorism sanctions designed to protect Americans from terrorist violence." ¶501. That number is plausible in light of $115 million in confirmed transactions for Hamas and

PIJ alone. ¶¶1263, 1267. Binance's assistance was "enough to fund thousands of attacks." ¶745. Courts find substantial assistance for far less. *See Bonacasa v. Standard Chartered PLC*, 2023 WL 2390718, at *14 (S.D.N.Y. Mar. 7, 2023) ($25 million); *Bartlett*, 2020 WL 7089448, at *15 ("millions of dollars").

Defendants' Presence: Plaintiffs are aware of *no* JASTA aiding-abetting cases in which the defendant was physically present at the attacks, which makes sense given JASTA's purpose of preventing terrorists from "rais[ing] significant funds" from parties who "contribute material support or resources"—activities nearly guaranteed to occur remotely from attacks. JASTA §§ 2(a)(3), 2(a)(6), 2(b); *e.g.*, *Bartlett*, 2020 WL 7089448, at *13 ("afford[ing] this factor little weight" under *Halberstam*); *see also Zobay*, 695 F. Supp. 3d at 350 ("ongoing business relationship" demonstrated "transactional[]" presence).

Relationship to the Terrorists: Hamas, Hezbollah, PIJ, al-Qaeda, ISIS, and the IRGC were all Binance's customers; Binance knew it or consciously avoided knowing it; and Binance conducted hundreds of millions of dollars in direct transactions with those terrorist groups. This is more than sufficient: A "direct relationship between the defendant and the FTO is not required," *Honickman*, 6 F.4th at 501, and a "commercial relationship," even if "indirect" to an FTO, is sufficient where the assistance is substantial, *Averbach v. Cairo Amman Bank*, 2022 WL 2530797, at *16 (S.D.N.Y. Apr. 11, 2022). In any event, this factor is afforded "low[er] priority" under *Halberstam*, 705 F.2d at 488, and is primarily "useful for determining the defendant's capacity to assist," *Honickman*, 6 F.4th at 500. Binance's capacity was substantial.

State of Mind: This factor concerns a "long-term intention to participate in an ongoing illicit enterprise." *Halberstam*, 705 F.2d at 488. It does not (*contra* Binance) require any "intention of facilitating" terrorist attacks. Rather it is "designed to capture the defendants' state of mind with

respect to their actions and the tortious conduct (even if not always the particular terrorist act)" to determine whether the defendant had "'some degree of knowledge that [its] actions [we]re aiding the primary violator.'" *Bonacasa*, 2023 WL 7110774, at *9 (quoting *Twitter*, 598 U.S. at 491, 503). Binance had such knowledge: It knew that FTOs operated on the Binance platform for years and that Binance's services were of particular utility in terrorist financing. *See supra* pp.10-13.

Duration: The duration of assistance speaks to whether it was intentional, or instead a mere "passing fancy" or "impetuous act." *Halberstam*, 705 F.2d at 488. Here, Binance provided unlawful assistance to terrorists for years, until enforcement actions caused it to stop—but Plaintiffs also allege that Binance's support for illicit customers is ongoing. *E.g.*, ¶765. This longstanding pattern weighs heavily in favor of liability.

IV. Plaintiffs State Conspiracy Claims

Under JASTA, "liability may be asserted as to any person ... who conspires with the person who committed such an act of international terrorism." 18 U.S.C. § 2333(d)(2). To state a JASTA conspiracy claim, a plaintiff must allege: "(1) an agreement between two or more persons; (2) to participate in an unlawful act; (3) an injury caused by an unlawful overt act performed by" a conspirator; (4) which "was done pursuant to and in furtherance of the common scheme." *Freeman*, 57 F.4th at 76-77 (quoting *Halberstam*, 705 F.2d at 477). Co-conspirators are "liable for all reasonably foreseeable acts taken to further the conspiracy." *Twitter*, 598 U.S. at 496. Plaintiffs allege each element.

Plaintiffs allege agreement and common purpose. Under *Freeman*, a JASTA conspiracy requires an agreement, which may be inferred from plausible allegations that the defendant and its co-conspirators "were pursuing the same object." 57 F.4th at 79-80. In the civil context, "[p]roof of a tacit, as opposed to explicit, understanding is sufficient to show agreement," and so "a civil conspirator can be liable even if he neither planned nor knew about the particular overt act that

caused injury, so long as the purpose of the act was to advance the overall object of the conspiracy." *Id*. at 77; *Gelboim v. Bank of Am. Corp.*, 823 F.3d 759, 781 (2d Cir. 2016) (noting that "conspiracies are rarely evidenced by explicit agreements" and "nearly always must be proven through inferences that may fairly be drawn from the behavior of the alleged conspirators"). Here, Plaintiffs allege an agreement and common objective for each conspiracy claim.

The Counterpressure Conspiracy (Count Two) alleges a conspiracy led by the IRGC and its terrorist proxies with a common objective of eliminating international sanctions on Iran by demonstrating that the sanctions are both ineffective and costly. ¶¶3054-56. The conspirators sought to achieve this by simultaneously "creating and using alternative financial systems that facilitated access to the U.S. economy without reliance upon the formal U.S. financial system" and supporting "terrorist attacks targeting the United States." ¶3056. Binance joined the conspiracy in or about 2018 "to be positioned to extract windfall profits … when U.S.-Origin Sanctions collapsed." ¶3098. To that end, it conspired directly with IRGC front Nobitex, "regularly communicat[ing] … and mak[ing] common cause" with "Nobitex personnel" to facilitate nearly $8 billion in Iranian cryptocurrency transactions that evaded—and thereby undermined—the sanctions regime. ¶¶3057-61. Similar allegations have sustained other JASTA conspiracy claims. *See King*, 2022 WL 4537849, at *10 ("The Complaints allege that Defendant took deliberate steps to help customers evade international sanctions regimes, and in doing so incurred business risk that ultimately led to Defendant's expulsion from the U.S. Those allegations are sufficient to make the plausible inference that Defendant had an agreement to further its customers' campaign of terrorism and shared a common purpose to do so.").

Binance fails to acknowledge these allegations. Instead, it argues that its mere "knowledge" of the conspiracy is not enough to infer an agreement. BHL Mem. 25-26. But Plaintiffs never

argued otherwise. Instead, they argue that Binance had knowledge of the conspiracy—and took repeated, robust action to assist the conspirators in their goals. This case is also different from other cases cited by Defendants, including *Freeman* and *Kemper v. Deutsche Bank AG*, 911 F.3d 383 (7th Cir. 2018), because Plaintiffs do not only allege a conspiracy to help Iran evade sanctions; they also allege that the underlying purpose of those violations was to advance Iran's counterpressure campaign—an allegation that no other court has rejected.

The Ransom Conspiracy (Count Three)[6] alleges that in 2017, Binance joined a conspiracy led by the IRGC and its terrorist proxies, the "overall object" of which "was to maintain each [terrorist group's] ability to access the payments they received in connection with their hostage-taking, human trafficking, ransomware, and protection payment schemes (collectively, 'Axis Payments')." ¶3134. Specifically, Binance joined the Ransom Conspiracy by agreeing with the IRGC through IRGC front Nobitex "to operate an illegal MTB" [money transmitting business] that helped the IRGC and its terrorist proxies to gather, process, and spend the proceeds of the Axis Payments. ¶¶3134-38. This conspiracy allegation is on all fours with *Halberstam*, where the defendant was liable for acting as the "secretary and recordkeeper" of transactions designed to "[d]ispos[e] of the loot" from her boyfriend's burglaries. 705 F.2d at 486. Just as the defendant in *Halberstam* was liable for willingly lending her back-office services to a burglar, Binance is liable for agreeing to help terrorists receive, move, and spend the proceeds of their various rackets.

Binance does not explain why these allegations do not sufficiently support an inference of agreement. It first argues that BHL did not have "any contact with Axis-affiliated terrorists." BHL Mem. 26. That is wrong, because part of the allegations underlying this conspiracy is that violent

[6] Binance refers to an "Axis Conspiracy," a term not used in the Amended Complaint. BHL Mem. 24, 26, 28. Plaintiffs assume references to the "Axis Conspiracy" refer to the Ransom Conspiracy.

terrorists actually used Binance wallets to receive, move, and spend the proceeds of their terrorist activities. ¶¶19, 580, 700-08, 720, 728, 761, 763-65, 767, 777-81, 1153, 1158. In any event, Binance's point is irrelevant under *Freeman*, which expressly rejected any requirement "that each member of a conspiracy conspire directly with every other member of it." 57 F.4th at 78. Binance next attempts to characterize its conduct as a mere "failure to implement adequate AML controls." BHL Mem. 26. But this is nothing more than a rehashing of its arguments, addressed in the aiding-and-abetting section, that its conduct was not culpable. In light of the allegations of active, culpable assistance recited *supra* pp.4-13, the Court cannot credit those arguments at the pleading stage. Finally, Binance asserts that it had no agreement with Nobitex to operate an MTB to process Ransom Payments (BHL Mem. 26)—but this is pure *ipse dixit*. Based on the tremendous volume of transactions Binance processed for Nobitex (almost $8 billion, *see* ¶763), the best inference is that Binance agreed to facilitate this institutional customer's unlawful transactions.

The ISIS Conspiracy (Count Four) alleges that Binance entered an agreement with ISIS in 2017 "with the overall goal of providing material support for ISIS in violation of 18 U.S.C. § 2339B." ¶3168. Binance's assertion that Plaintiffs' claim should be dismissed because it relies on Binance's "routine transaction services to individuals or entities that Plaintiffs later connected to ISIS," BHL Mem. 27, is wrong for multiple reasons. First, Plaintiffs squarely allege that Binance's illegal dealings were *not* "routine business transactions." *See supra* p.20. Second, Plaintiffs extensively allege that Binance did business with ISIS knowingly or with conscious disregard for that fact, *e.g.*, ¶¶1486-89, and Binance makes no attempt to explain why those allegations are implausible.

JASTA conspiracy does not require that the object of the conspiracy be terrorism. JASTA conspiracy does *not* require that "the goal of the conspiracy" be to "commit an act of

international terrorism." *Contra* BHL Mem. 27-28. Any such requirement would clash with *Halberstam*, where the defendant was found liable for conspiring in Halberstam's murder despite lacking any intention to commit murder. 705 F.2d at 487. It is also contrary to *Twitter*, which reaffirmed *Halberstam*'s principle that "conspiracy liability could be premised on a 'more attenuated relation with the principal violation' because the defendant and the principal wrongdoer had agreed to a wrongful enterprise," and that such liability extends to all foreseeable consequences of acts taken in furtherance of the conspiracy. 598 U.S. at 490 n.9. The Second Circuit's decision in *Freeman* does not hold otherwise. Indeed, in *Freeman* itself, the defendants urged the same rule as Binance does now,[7] but the Second Circuit rebuffed it. Rather, the court concluded that where the plaintiffs alleged that the terrorists' goal included "planning and perpetrating the murder and maiming of hundreds of Americans in Iraq" but the defendant bank's goal did not, there was no *common* objective sufficient to support conspiracy liability. *Freeman*, 57 F.4th at 80. That case is inapposite here because Plaintiffs identify alternative objectives—the counterpressure campaign, processing ransom payments, and supporting ISIS—that were shared by the terrorists and Defendants.

Plaintiffs allege overt acts in furtherance of the conspiracies. All Plaintiffs' injuries "were caused by an unlawful overt act done in furtherance of the conspirators' common scheme"—specifically, acts of international terrorism. *Freeman*, 57 F.4th at 80. For each conspiracy, Plaintiffs explain how the terrorist attacks that injured Plaintiffs furthered the conspiracy. For the Counterpressure Conspiracy, the conspiracy's objective was to eliminate or degrade U.S. and international sanctions, which the conspirators sought to achieve by demonstrating that sanctions

[7] Brief for Defendants-Appellees at 15, *Freeman v. HSBC*, No. 19-3970 (2d Cir. May 18, 2020) ("A complaint asserting a JASTA conspiracy claim must allege that the defendant agreed to further the terroristic goals of the person who committed the underlying terrorist act.")

were ineffective in: (1) preventing the terrorists' access to the international financial system; and (2) preventing terrorist attacks, which escalated in response to sanctions. Binance served the former role; the terrorist attacks on Plaintiffs served the latter. ¶¶3111-20; *see also, e.g.*, ¶¶1589, 1691, 2280, 2339, 2367, 2377, 2405, 2481, 2678, 2922, 3031, 3093.

Terrorist attacks furthered the Ransom Conspiracy because the conspiracy centered on facilitating and monetizing specific types of terrorist financing payments, including hostage-taking ransoms and protection payments. ¶¶3134-37. These required actual terrorist attacks to generate the payments that would then flow through the Binance-Nobitex payment channels established as part of the conspiracy. *See id*. The attacks also demonstrated "the IRGC's continuing ability to credibly threaten and/or commit an act of terrorism," which was "vital to the IRGC's [and] Binance's … ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence." *Id*. ¶1590; *see also, e.g.*, ¶¶1642, 1692, 2140, 2210, 2324, 2407, 2588, 2601, 2703, 2855. The attacks thus directly advanced the conspiracy's core object of generating and monetizing terrorism-related payments.

Plaintiffs also allege in detail how ISIS attacks on Plaintiffs were acts in furtherance of the ISIS Conspiracy, because terrorist "[v]iolence created the demand and transaction activity that drove ISIS's, [and] Binance's … ability to mutually benefit from their participation in the ISIS Conspiracy." ¶2932; *see also* ¶¶2976, 3001.

Binance's treatment of the "overt act" requirement merely reiterates its contention that the object of a JASTA conspiracy must be "to commit an act of international terrorism." BHL Mem. 28-29. As explained *supra*, that argument is wrong, and Binance has offered no other basis for finding Plaintiffs' allegations of "overt acts" inadequate.

V. Plaintiffs State A Primary Liability Claim Based On Terrorist Ransomware Attacks

Finally, Plaintiffs allege that Defendants themselves committed an act of international terrorism by providing material support to the cyberterrorist organization Wizard Spider in violation of 18 U.S.C. § 2339A. Specifically, Wizard Spider—also known as TrickBot and Conti group—is a state-sponsored cyberterrorist group that emerged in 2017, committing "a wave of terrorist attacks targeting the United States." ¶1519. Wizard Spider's ransomware operations targeted hospitals in the United States; the organization inserted malware into hospitals' information technology systems, causing those systems to fail unless the terrorists' demands (for money) were met. *Id*. In carrying out these attacks, Wizard Spider "leveraged the certainty that a patient would eventually die to coerce such hospitals to yield to the terrorists' demands." *Id*. In particular, Wizard Spider used a ransomware software strain called Ryuk, which employed code shared between and amongst North Korean and Russian government actors. ¶1521.

For ransomware schemes to work, terrorists need to obtain and escape with the ransom money. "Binance served as the destination-of-choice for cybercriminals to cash-out ransom payments generated from their attacks. This was well-known to Binance and Zhao." ¶1526; *see also* ¶¶777-80, 1532-48 (detailing Binance's participation in IRGC and North Korean ransomware schemes). Indeed, Binance "was aware of the significant uptick in ransomware activity on the exchange as early as February 2019." ¶1528. In 2020, researchers "found that bitcoin worth over $1 million from several addresses connected to Ryuk ransomware attacks made its way to a wallet on the Binance exchange over the last three years." ¶1526. In its settlement with FinCEN, Binance admitted that it was a "direct counterparty with ransomware-associated addresses in hundreds of transactions." ¶1527. But even though "Binance was aware of many specific movements of ransomware proceeds through the platform," it "failed to file SARs with FinCEN." ¶1528. This included "transactions [Binance] processed involving the Conti group," *i.e.*, Wizard Spider. ¶1529.

Binance was aware of these transactions because it received "reports from [its] third-party service providers about such attackers using the Binance platform," which "included specific CVC wallet addresses and methodologies associated with over $12 million of CVC that traced specifically from [Wizard Spider] attackers to accounts at Binance." *Id*. Based on reports from the blockchain analysis firms TRM Labs and Elliptic, Plaintiffs allege that "Defendants enabled Wizard Spider to conduct *over $16 million* in transactions on the Binance exchange." ¶1530.

By playing the role of a virtual bag-man for ransomware attacks, Binance played an essential role in those attacks. "Binance's actions were a but-for cause of the effectiveness of, and harm caused by, each such Wizard Spider attack." ¶1531. Plaintiffs further allege that Wizard Spider members were treated as VIP customers by Binance. ¶3182. By maintaining wallets and processing transactions for attacks that threatened human lives, Defendants provided material support to the organization that carried out those attacks. ¶3181. What is more, "Wizard Spider executed ransomware attacks at least in part to raise money to fund future attacks" by funding "recruitment and retention," "developing and deploying original ransomware software," and "maintaining a massive robot network" to deploy in its attacks. ¶1522. Thus, Binance's participation in Wizard Spider attacks also enabled future attacks.

This included the July 2019 attack on the Springhill Medical Center in Mobile, Alabama. ¶1523. Wizard Spider attacked that hospital using the Ryuk ransomware strain, seeking payments "to end the attack that were intended to flow to Binance's exchange." ¶1524. The attack caused the death of an infant—whose estate and bereaved mother bring a claim for primary liability. ¶¶3023-28, 3033-40, 3180, 3186.

This claim is different in kind from the primary liability claim rejected in *Raanan*. There, the Court acknowledged that "primary liability may … lie where banking services are directed at

a specifically identifiable violent or dangerous act." 2025 WL 605594, at *16. But the Court reasoned that the general provision of financial support was not enough. Plaintiffs' claim does not rest on the general provision of financial support. Instead, it arises from Binance's direct participation in a ransomware scheme routinely used to disrupt critical U.S. hospital systems.

Binance responds that "providing ordinary business services to a terrorist organization is not sufficient to plead a violent act." BHL Mem. 14. But knowingly participating in ransomware schemes is not "ordinary business." Courts have held that payments directed to a terrorist organization's violent activities are "dangerous to human life" and thus satisfy the definition of international terrorism. *Boim*, 549 F.3d at 690; *In re Chiquita Brands Int'l, Inc.*, 284 F. Supp. 3d 1284, 1316 (S.D. Fla. 2018); *Wultz v. Islamic Republic of Iran*, 755 F. Supp. 2d 1, 44 (D.D.C. 2010). That makes sense: Absconding with the ransom is an essential component of a ransomware attack—and if the attack as a whole is dangerous to human life, its essential components are, too. There can be no doubt that ransomware attacks on hospitals—one of which caused the tragic death of a child—endanger human life.

Defendants argue next that the complaint does not allege that Binance knew or intended that its support would be used to carry out a criminal act, as required by 18 U.S.C. § 2339A. BHL Mem. 14-15. But Plaintiffs allege enough to support an inference of knowing complicity at the pleading stage. Binance was "the cyber criminals' exchange of choice." ¶1526. Alongside other allegations of knowledge, ¶¶1526, 1528-29, 3183, Plaintiffs allege that Binance was aware of a significant uptick in ransomware activity on its exchange as early as February 2019—months before the attack in question, ¶1528. What is more, Binance treated Wizard Spider customers as VIPs, served as a direct counterparty for ransomware wallets in many transactions, and consciously

moved millions of dollars for ransomware operators including Wizard Spider without ever reporting such transactions to authorities. ¶¶1518, 1529-31.

Binance argues next that there was no objective terroristic intent. BHL Mem. 15-16; BAM Mem. 25. As Binance recognizes, this is an objective inquiry—and so the question is whether the ransomware attack objectively appeared calculated to intimidate or coerce a civilian population, and not what Binance subjectively believed. Yet Binance's argument is entirely about whether it had subjective knowledge (a contention addressed in the previous paragraph)—not whether an objective observer would conclude that one participating in a ransomware attack on a U.S. hospital by a state-sponsored terror group had terroristic intent. On the latter point, the complaint's allegations are unrefuted and logical: An attack on a civilian hospital designed to force it to pay a ransom clearly exhibits objective terroristic intent. ¶¶1519-21, 3184.

Finally, Binance disputes proximate causation. BHL Mem. 16-17. But Binance's objection here is a factual one. Plaintiffs allege that "Binance's actions were a but-for cause of the effectiveness of, and harm caused by, each such Wizard Spider attack." ¶1531. That is because "Wizard Spider relied upon Binance's exchange to accept payment to end its attacks," and as a matter of "custom and practice, and tactics, techniques, and procedures," routed ransom funds "to one or more Wizard Spider wallets on the Binance exchange." *Id.* Those funds related to attacks beginning in 2017—and the proceeds were used "at least in part to raise money to fund future attacks." ¶¶1522, 1525. Binance responds that Plaintiffs do not link any specific transaction to the 2019 attack at issue—but Plaintiffs explain both that the proceeds of prior attacks funded subsequent attacks and also that the availability of a destination for ransom funds was critical to the success of every ransom attack. ¶¶1522, 1531. That is enough to plead proximate cause.

CONCLUSION

The Court should deny the motions to dismiss.

Respectfully submitted,

/s/Tejinder Singh

Ryan R. Sparacino (pro hac vice)
Geoffrey P. Eaton (pro hac vice forthcoming)
Matthew J. Fisher (pro hac vice)
Adam J. Goldstein
Tejinder Singh
SPARACINO PLLC
1920 L Street, NW, Suite 835
Washington, D.C. 20036
Tel: (202) 629-3530
ryan.sparacino@sparacinopllc.com
geoff.eaton@sparacinopllc.com
matt.fisher@sparacinopllc.com
adam.goldstein@sparacinopllc.com
tejinder.singh@sparacinopllc.com

Vincent Levy
HOLWELL SHUSTER & GOLDBERG LLP
425 Lexington Ave., 14th Floor
New York, N.Y. 10017
Tel: (646) 837-5151
vlevy@hsgllp.com